



Wireless Endpoint Security



www.airpatrolcorp.com

I. Introduction

To enhance productivity and efficiency, employees are increasingly turning to wireless networks to get the job done. The security experts at AirPatrol believe that a defense-in-depth approach to wireless security yields the greatest results, especially when it comes to protecting corporate laptops. Armed with AirPatrol's endpoint security solution, an IT administrator can ensure the proper use of wireless laptops for those users on the go. At the center of AirPatrol's protection suite is its Wireless Endpoint Client software (WEC); a small application that runs as a system service on wireless laptops. WEC protects the laptop by strictly defining how the wireless interface will be used. The policy defining wireless usage can be as flexible or rigid as the corporate security policy dictates. By leveraging Microsoft's Active Directory and AirPatrol's native Wireless Policy Manager (WPM), the Wireless Endpoint Client (WEC) can begin to ease the burden of managing and securing wireless assets.

II. Wireless Endpoint Client

WEC – Wireless Policy Manager Version

Enhanced wireless security policies can also be centrally managed using AirPatrol's Wireless Policy Manager (WPM). Based on the JBoss application server, WPM is a web-based server application that allows wireless security policy to be easily designed and effectively deployed. WPM is capable of delivering more granular wireless usage policies and USB device control capabilities than that of standalone WEC.

Ease of Deployment

The foundation for building a secure wireless endpoint solution begins with the understanding of three configuration concepts: Users, Groups, and Policy. WPM utilizes Microsoft's Active Directory (AD) to ease the burden of managing a large deployment of WEC across the enterprise. WPM can query AD to build a subscriber list of users that wireless security policy will apply. In addition, AD can distribute WEC to those wireless laptops where wireless security policy should be enforced. The WEC installation package can be published across AD using a Group Policy MMC. Simply create a Group Policy Object that installs the package when the users next log in.

Scalability

With ease of use and scalability at the center of its design, a single instance of WPM can manage up to 10,000 WEC deployed endpoints. Larger managed installations of WEC (50,000 or 100,000 WEC deployed endpoints) are feasible by using redundant WPM servers in a load-balanced configuration.

Security

All of AirPatrol's products undergo rigorous software security testing. All the underpinnings of WPM are security hardened to greatly reduce the attack surface of the application. Moreover, all network communications between WPM and WEC are fully encrypted. Once installed, the IT administrator simply opens a secure HTTPS connection to WPM using a standard web browser. Once successfully authenticated, the task of designing wireless security policy is underway. Just as HTTPS is used to secure connections between an administrator's web browser and WPM, the same secure SSL based communications paradigm is used for all communications between WPM and WEC. This ensures the

confidentiality and integrity of the policy data as it travels over the network. WPM based wireless security policies include:

- **AirSafe** – Automatic, out-of-the-box protection against multi-homing. 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. This completely mitigates the possibility of bridging a potentially untrusted wireless network with a trusted corporate wired LAN. In addition, this protection is carried over into the realm of cellular broadband connections and traditional 802.11 networks. Should WEC detect an active cellular broadband connection it will automatically disable the wireless adapter.
- **802.11 Infrastructure Authentication policy enforcement** – WEC allows the system administrator to define minimum levels of security that must be used when connecting to wireless networks.
- **802.11 AdHoc Authentication policy enforcement** – WEC allows the system administrator to set minimum levels of security used, or completely disable the use of AdHoc wireless networks.
- **Virtual Private Network (VPN) policy enforcement** – The ability to force the use of a VPN within a specified amount of time. If a VPN connection is not made within the specified interval, wireless network connectivity is terminated protecting the laptop from a potentially unsecure wireless network.
- **Connection Exceptions** – Allows the administrator to create either a list of permitted or disallowed wireless networks. The network SSID must be present (white list) or not be present (blacklist) in order to allow wireless network connections.
- **Endpoint Firewall** – The ability to enforce the use of a host-based endpoint firewall prior to allowing wireless network connections.
- **Location Aware** – The ability to predefine a list of trusted, preferred wireless networks that will be made exclusively available for connection when their presence is detected by WEC. This ensures connectivity control whenever corporate laptops are within range of corporate wireless access network while preventing accidental or intentional wireless connections to uncontrolled (rogue) access points residing off premise.
- **USB Device Control** – Provides the capability to control what types of USB devices can connect to the WEC enable laptop. For example, the user may be allowed to connect a USB capable mouse while USB mass storage devices are disallowed.

III. System Requirements

WEC

Once installed the overall footprint and processor consumption of WEC running on a laptop or wireless workstation is minimal. The installed package uses only 16MB of system memory along with 4MB of hard disk space. This is the same for both the standalone version of WEC and the WPM managed version. The host platform running the WEC client must meet the following minimum requirements:

- 1000 MHz Pentium class machine or better
- 128 MB of RAM or higher
- Ethernet 10/100 Network Interface Card (NIC)
- NDIS 5.1-compliant wireless adapter and driver
- Cellular card (optional), Please refer to the list of supported cellular devices on the Wireless Endpoint Client product page <http://www.airpatrolcorp.com>
- Microsoft Windows® XP (32 bit only) or Windows® Vista. Windows® 7 support will be available mid September, 2009.

Wireless Policy Manager

The host platform running WPM must meet the following minimum requirements in order to manage up to 10,000 WEC endpoints:

- Quad Core 2.6 GHz Pentium Class Processor
- 4 GB of RAM or higher
- 10 GB of hard disk space or greater
- Microsoft Windows® XP Professional Edition (SP2) or Microsoft Windows® 2003 (SP4)

IV. Summary

At AirPatrol, we believe that wireless and security are not mutually exclusive terms. Armed with the proper tools, IT departments can effectively manage and mitigate wireless risks while supporting all the benefits that wireless networking offers.

AirPatrol's Wireless Endpoint Client (WEC) plays an integral part in any organization's approach to enforcing wireless security policy. Whether an IT department is responsible for only small number of wireless laptops or tens of thousands of wireless laptops, AirPatrol's Wireless Policy Manager and Wireless Endpoint Client together facilitate the secure use of these valuable assets.

About AirPatrol Corporation

As the most trusted authority on wireless threats to wired and wireless networks, AirPatrol Corporation delivers the security and network management capabilities today's businesses and government agencies require to solve the industry's most pressing wireless security and network management issues. By offering a comprehensive suite of wireless threat management solutions, AirPatrol enables entities to keep pace with the expanding requirements of a mobile world while complying with pertinent regulations and protecting communications, critical information, and IT infrastructure against present and future wireless threats. Customers and partners include leading network infrastructure and wireless vendors, Fortune 100 enterprises and high-profile government agencies around the globe.

For more information about the contents of this white paper, AirPatrol Corporation products or our company, please contact us at info@airpatrolcorp.com or call us at +1-866-430-4227.