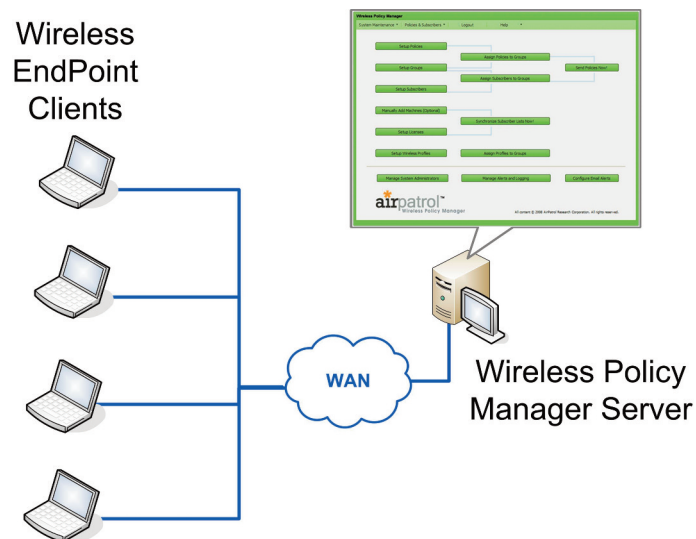


Wireless Policy Manager

Over 500 million wireless laptops are currently in use – each susceptible to wireless attacks. With over 100 million more shipping each year, it's critical for network administrators to have the right tools to enforce endpoint security, whether they have a planned wireless network or not.

Wireless Policy Manager offers proven, award-winning protection so organizations can efficiently manage security for their wireless-enabled endpoints and gain confidence that corporate assets and business operations are protected — all while controlling costs.



Create Policies and Maintain Industry Compliance

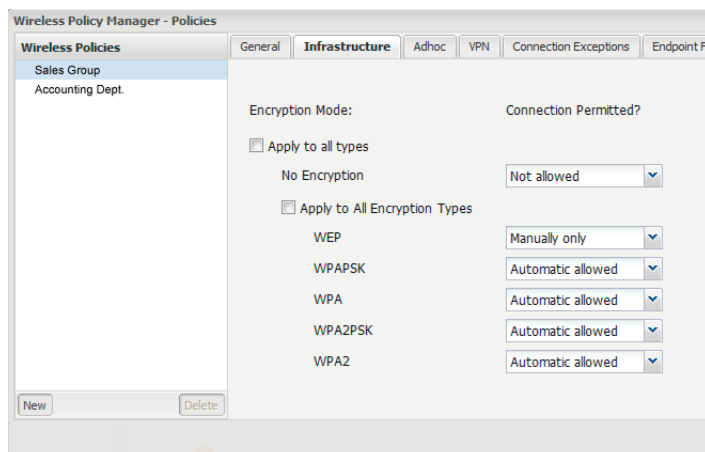
Wireless Policy Manager enables administrators to easily enforce critical wireless and USB security policies on their enterprise endpoints. Using the intuitive Wireless Policy Manager interface, network administrators define wireless and USB connectivity policies that control how, when, where and if users can connect to wireless networks and USB devices. WPM satisfies requirements mandated by government and industry such as FISMA, NIST, DoD, PCI, HIPAA, SOX, and GLB Standards. With WPM, IT Administrators efficiently secure endpoints and ensure standards compliance using tailored policies and automated reporting tools.

Streamline Administration of EndPoint Security

Through seamless integration with AirPatrol's Wireless EndPoint Client, administrators efficiently enforce wireless and USB connectivity best practices to provide comprehensive endpoint protection for business communications, critical information, and IT infrastructure.

Key Benefits and Features

- Manage endpoints from a centralized Administrator's console
- Control how, when, or where users establish wireless connections
- Prevent wireless bridging, ad-hoc connections, and more
- Ensure that users only operate approved USB hardware
- Set minimum security requirements for wireless connections
- Disable connections to potentially dangerous SSIDs
- Customize policies based on location
- Require use of VPNs or other security measures
- Control USB connectivity, including Thumbdrive, BlueTooth, WiFi, and Cellular Broadband devices



AirPatrol Corporation

9861 Brokenland Parkway
Suite 204
Columbia, MD
21046 USA
Phone: 1-866-430-4227

info@airpatrolcorp.com
www.airpatrolcorp.com

Wireless EndPoint Client

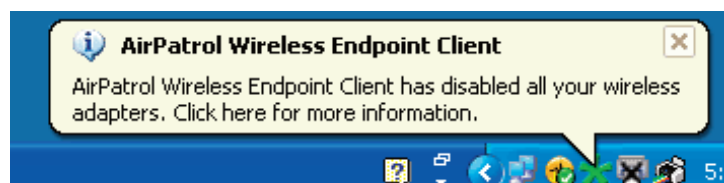
Securing mobile wireless endpoints is more complex than ever. External threats such as wireless phishing, rogue access points, malicious code, and even end-user mistakes can place business communications and critical IT infrastructure at risk.

Used in conjunction with Wireless Policy Manager, AirPatrol Wireless EndPoint Client helps enforce corporate wireless and USB security policies while protecting wireless endpoints against known and unknown threats - without inhibiting users or slowing performance.

Wireless EndPoint Client

Prevent Wireless Vulnerabilities

Whenever a laptop makes a wired network connection, Wireless EndPoint Client immediately disables all wireless interfaces on the laptop using AirPatrol's AirSafe™ technology. This prevents multi-homing at the access layer of the corporate network and mitigates the risks associated with bridging networks that can result in a network breach.



Cellular Card and Modem Control

AirPatrol's Wireless EndPoint Client can also disable and enable your cellular card or modem whenever it detects wired or wireless connections. When your cellular card or modem are active, AirPatrol Client will automatically disable your wireless adapter.

Control Connections with Location Aware

AirPatrol's Location Aware technology enhances wireless endpoint security by forcing all wireless communications toward a predefined and authorized list of corporate access points anytime those networks are within range. This prevents users from connecting to unknown, potentially dangerous access points, anytime your corporate wireless network is available.

Define and Enforce

WPM and WEC allow you to define and enforce a variety of wireless and USB security policies, including:

- **AirSafe™**
Automatic, out-of-the-box protection against multi-homing. When a laptop's wireless interface (802.11 card OR cellular broadband modem) is active and a wired Ethernet connection is attempted, AirSafe™ automatically disables the wireless connection.
- **802.11 Infrastructure Authentication**
Set minimum levels of security to be used when connecting to wireless networks.
- **802.11 AdHoc Authentication**
Set minimum levels of security (or completely disable) AdHoc networks.
- **Virtual Private Network (VPN)**
Force a VPN connection within a specified amount of time.
- **Connection Exceptions**
Create a list of permitted or disallowed wireless networks.
- **Endpoint Firewall**
Enforce the use of a host-based endpoint firewall prior to allowing wireless network connections.
- **Location Aware**
Predefine a list of trusted, preferred wireless networks that will be made exclusively available for connection when detected by WEC. This ensures connectivity control whenever corporate laptops are within range of the corporate wireless network. Prevents accidental or intentional wireless connections to rogue access points residing off-premise.
- **USB Device Control**
Control what types of USB devices can connect to the WEC-enabled laptop. (e.g. allow a USB capable mouse but disallow USB thumb drives or Bluetooth devices)

AirPatrol Corporation

9861 Brokenland Parkway
Suite 204
Columbia, MD
21046 USA
Phone: 1-866-430-4227

info@airpatrolcorp.com
www.airpatrolcorp.com