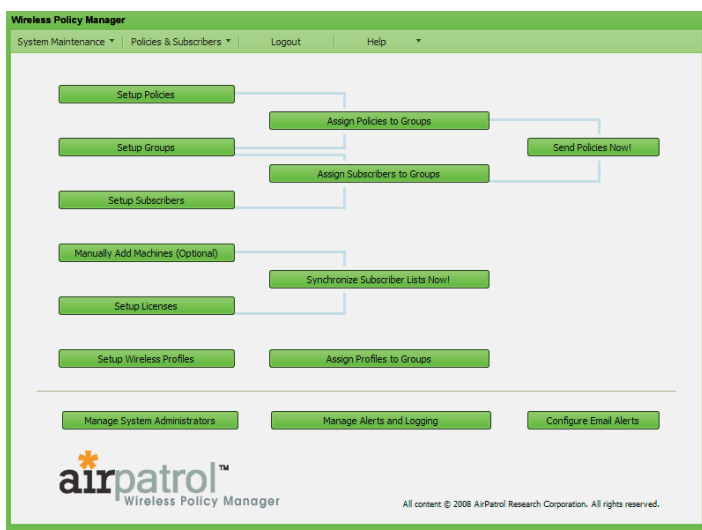


# Wireless Policy Manager

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

Wireless Policy Manager offers proven, world-class protection without added resources, so organizations can efficiently manage security for all wireless-enabled endpoints and gain confidence that corporate assets and business operations are protected — all while controlling costs.



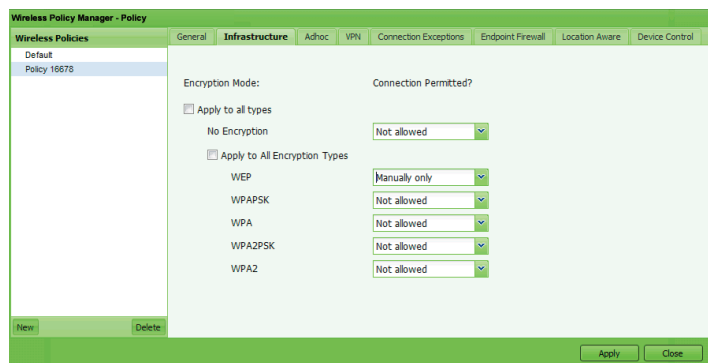
## Create Policies and Maintain Industry Compliance

Wireless Policy Manager allows administrators to create security policies for laptops and mobile devices and maintain compliance with industry regulations.

Using the intuitive Wireless Policy Manager interface, network administrators can define wireless connectivity policies to control how, when, where and if users can connect to wireless networks. Policies can be documented as required to comply with industry mandates such as Health Insurance Portability and Accountability Act (HIPAA)", Sarbanes-Oxley Act (SOX), and Payment Card Industry (PCI) using the convenient reporting tools.

## Streamline Administration of EndPoint Security

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



## Key Benefits and Features

- Efficiently manage endpoint security from a single interface
- Control how, when, or where users establish wireless connections
- Prevent wireless bridging, ad-hoc connections, and more
- Ensure that users only operate approved 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

## AirPatrol Corporation

### Public Sector Sales:

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

### Research & Development:

203-8525 Baxter Place  
Burnaby, BC  
V5A 4V7  
Canada  
Phone: 604.298.4227

info@airpatrolcorp.com  
www.airpatrolcorp.com

# Wireless EndPoint Client

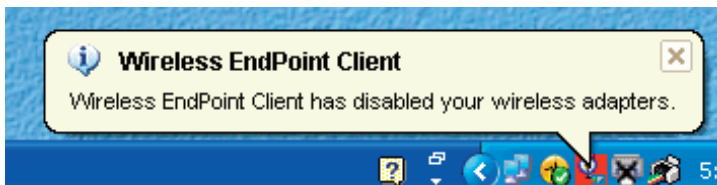
Securing wireless endpoints that travel outside the office is more complex than ever. Hackers, malicious code and end-user mistakes can place business communications, critical infrastructure, and IT infrastructure at risk.

**AirPatrol Wireless EndPoint Client helps enforce corporate wireless security policies while protecting wireless endpoints against known and unknown threats without inhibiting users or slowing performance.**

## Wireless EndPoint Client: Stand-Alone Edition

### Prevent Wireless Hacking

To prevent wireless hacking at its source, Wireless EndPoint Client automatically turns off the wireless adapter whenever a laptop is connected to a wired network port. This addresses the security deficiencies in standard Windows® XP and Vista wireless clients and prevents Wi-Phishing attacks that enable a hacker to bridge the connection between a wireless laptop and the corporate wired network.



### 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.

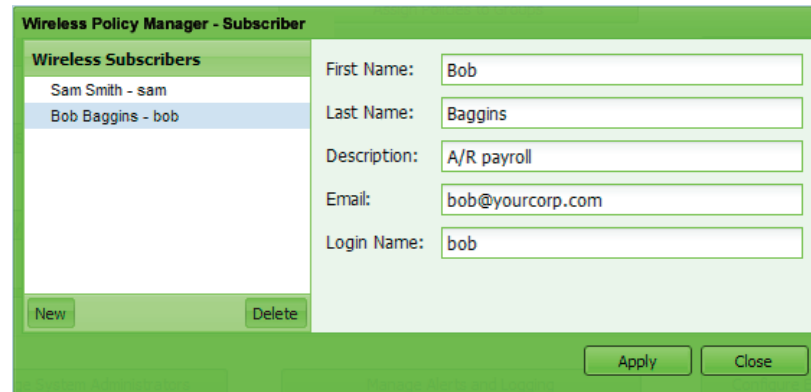
### Control Connections with Location Aware

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.

## Wireless EndPoint Client: Policy Manager Edition

### Enforce Wireless Connectivity Best Practices

Wireless Policy Manager (WPM) puts the wireless administrator back in the drivers seat when it comes to endpoint security. With an easy to use, intuitive user interface and rapid deployment, WPM provides a framework that delivers best of breed wireless security practices to corporate assets. WPM seamlessly protects business communications, critical information, and IT infrastructure and controls how, when, and if a user can connect to the corporate wireless network.



When used in conjunction with AirPatrol's Wireless Policy Manager, Wireless Endpoint Client offers secure endpoint protection, including AirPatrol's Location Aware feature, and cellular broadband, modem, and USB device control, along with comprehensive wireless policy management and enforcement capabilities.

## AirPatrol Corporation

### Public Sector Sales:

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

### Research & Development:

203-8525 Baxter Place  
Burnaby, BC  
V5A 4V7  
Canada  
Phone: 604.298.4227

info@airpatrolcorp.com  
www.airpatrolcorp.com