- Enforce wireless security policy for mobile devices when at home, hotels, airports, hot spots or any other non-corporate location
- Prevent wireless threats including ad hoc networking, Evil Twin/honey pot access point connections and Wi-Phishing
  - No open network usage
  - Enforces VPN connectivity for any non-enterprise network
  - Prevents bridging between wireless and wired network interfaces
  - Prevents multiple simultaneous network interfaces
- Automatic notification of all wireless client vulnerabilities while away from the office
- Central management and disbursement of security policies by user type/group
  - Ability to automate SAFE deployments to 1000s of laptops
  - Policy enforcement for all wireless interfaces

SpectraGuard® SAFE

Wireless Security Agent For Endpoints (SAFE)

Protect mobile clients from wireless threats – 24x7

Protect Mobile Clients from Wireless Threats – 24 x 7, wherever they are

Business today requires network and email connectivity around the clock and around the globe. Laptops and their users are mobile. They require connectivity in the office, on the road, and at home – and more than half the time when they are mobile, they are on wireless connections.

WLAN connectivity while convenient and easy to use, also creates a number of security risks for the laptop as well as the network. While the laptop is in a corporate facility – it can be protected by a wireless intrusion prevention system (WIPS). However, when it's out of the office, the only protection that can work is software on the laptop itself.

To provide this functionality, AirTight Networks provides SpectraGuard SAFE (Security Agent For Endpoints).

- Lightweight software agent that runs on mobile devices
- Prevents use of insecure wireless networks
- Protects against common wireless threats such as ad hoc networking, Evil Twin/honeypot access points and Wi-Phishing
- Protects against accidental / unintentional wireless connections - to popular SSIDs - without user knowledge
- Enhances security provided by mobile device firewall, anti-virus and VPN software
- Managed and enforced from a central location

Detect, Prevent Wireless Threats to Laptops

Microsoft designed Windows to be promiscuous, connecting easily over the air to any other wireless device or network that it detects. While this makes it easy to use, it creates three categories of security risk:

- connection to unsafe devices/networks
- open, unencrypted, unsecured communication
- unauthorized connectivity (bridging) back through the laptop to the enterprise intranet

Common Laptop Wireless Threats: Ad-hoc (PC to PC) Networking and Connection to Insecure Networks

These behaviors can lead to a loss of employee time and productivity, User ID and password theft, confidential data loss, network compromise, and the potential introduction of spyware, mal-ware, or other noxious software into your network. SpectraGuard SAFE protects your laptops against these threats.

Location Based Wireless Security

SpectraGuard SAFE allows the administrator (and/or user) to configure and manage distinct security profiles – for when their laptops are at:

- work
- home
- away

You can also define additional security profiles

Automatic Switching and profile based on network connection. For each of these profiles, the laptop can be instructed to:

- allow or disallow wireless connections in general, including 802.11 (a/b/g/n), Bluetooth, infrared, and 2.5/3G (GPRS, CDMA, EV-DO, EDGE, HSPRA, WiMAX etc.)
- allow connectivity only to specified APs,
- allow or disallow wired network connections, including: Ethernet, Firewire, dial-up modems
- require specific WLAN encryption requirements before allowing connection,
- allow or disallow networking behaviors related to wireless, such as
  - multiple simultaneous network connections
  - bridging between network interfaces
  - ad-hoc networking

So, for example the administrator can configure their laptop security policy to only allow connection to

- the authorized corporate WLAN with strong encryption (WPA2 or 802.11i) while in the office,
- the user's home AP with WEP encryption while at home
- only to certain ISPs/hot spots while traveling - and then to require a VPN connection while using these services or to only EVDO while on the road, disabling 802.11.

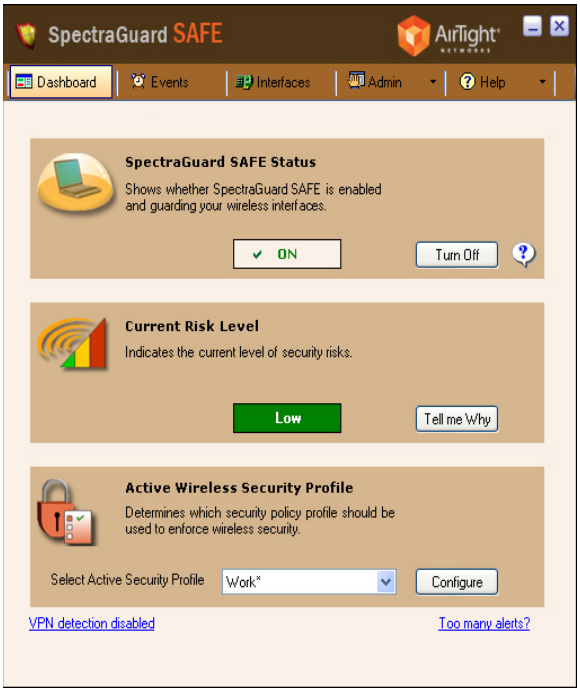
The administrator can lock down allusage profiles or allow users to modify selected profiles.

Friendly, Easy to Use User Interface

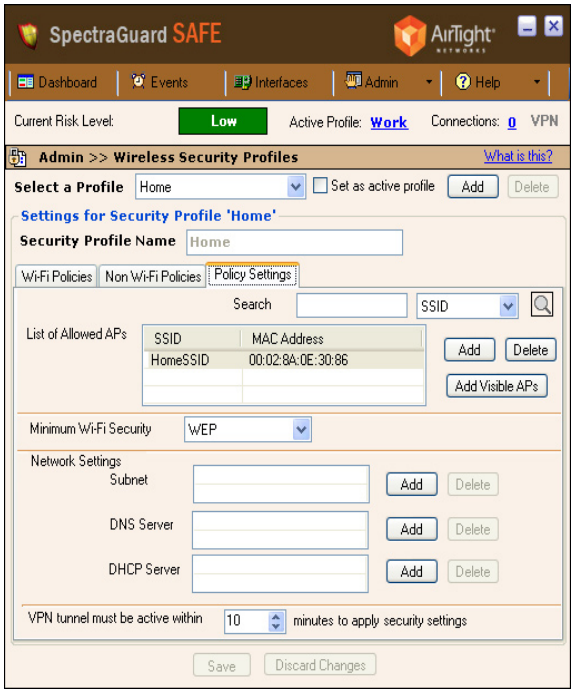
All of these features are made easy-to-use through a web-based graphical user interface (GUI) that walks the user through both configuration and set-up – and then through security alerts and troubleshooting if this is ever required.

Enforce Corporate Wireless Connectivity Security Policy on Mobile Devices

With SpectraGuard SAFE, and



SAFE Dashboard - simple, friendly user interface



Configuration screen for each usage profile: work, home, and away

SpectraGuard Enterprise – the corporate network administrator can configure and manage the wireless connectivity and security policies for all of the laptops in the enterprise. You can set location specific policies for wireless connections when the user is in the office, traveling, and at home.

Implement Different Security Policies for Different Groups of Mobile Users

SpectraGuard SAFE also allows different wireless security policies for different groups of users. The sales team is usually the team that requires the most flexible connectivity, whereas the finance department might have their laptops locked down to prevent loss of confidential financial data.

Require VPN Usage

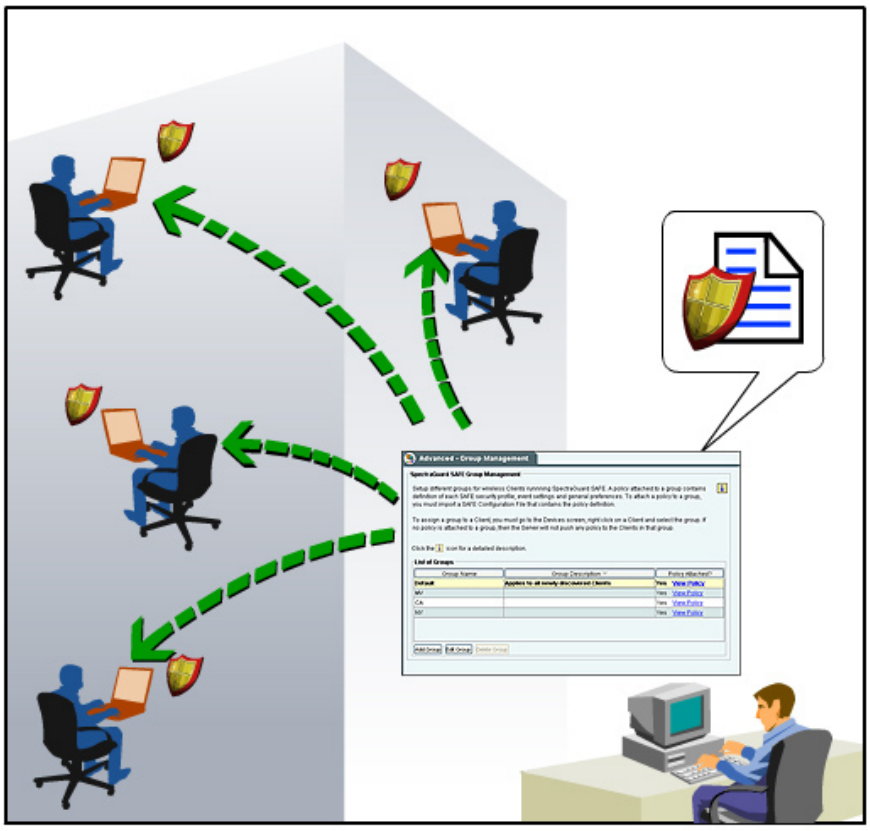
SpectraGuard SAFE also allows you to require the usage of a VPN client while on a wireless connection (such as a WiFi HotSpot) – when you're out of the office or a daily connection or a WiMAX connection

Protect the Enterprise Network from Clients that have been Compromised

SpectraGuard allows the network administrator to monitor the wireless behavior of employees' laptops – when they're out of the office. When they return to the office and connect back to the corporate network, a log file of the APs and devices to which they have connected is sent back to the SpectraGuard Enterprise. The administrator can then scan this list, and if suspicious, abnormal, or high risk behavior is detected then the administrator can take appropriate actions - such as educating the user, disabling wireless on that laptop, and/or invoking an inspection of that machine's software (using the appropriate tools).

Easy to Deploy

SpectraGuard SAFE deployment can be automated for 1000's of laptops using



Enterprise Edition provides central definition and enforcement of laptop wireless policies and behavior.

IT asset management systems such as Microsoft SMS or Altiris. IT administrators can package SAFE software along with pre-defined security configurations and push this out to their enterprise laptops. This installation can be hidden from the user (silent install). SAFE Upgrades can also be administered the same way.

Easy to Manage

SpectraGuard SAFE is easy to manage for the administrator through a webbased GUI that is an integral part of SpectraGuard Enterprise. Alerts, reports, and policies all can be managed for thousands of devices from a single SpectraGuard appliance, and with SpectraGuard MNC – a network of millions of wireless laptops can be secured.

Audit Wireless Usage/Generate Compliance Reports

SpectraGuard SAFE also provides simple, concise reports on all the laptops that it is protecting. The administrator can view the risk level (i.e. wireless Security threat index) for each user and can generate reports with the click of a button. SAFE client reports provide detailed log on wireless usage, reasons for risk level, and detailed list of wireless incidents on each user's laptop.

SpectraGuard SAFE

A simple, effective tool for protecting your enterprise's laptops from wireless threats – wherever they roam.

ABOUT AIRTIGHT NETWORKS

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WVM) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 11 U.S. patents and two international patents granted (UK and Australia), and more than 25 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA.

Specifications

Feature Specifications	
Enable/Disable SpectraGuard SAFE	• Enabled when system boots up • Users disallowed from disabling SAFE
Security Profiles	• Multiple Profiles (Work, home, away) • Automatic profile switching
Network Interfaces	Policy enforcement provided for: • Ethernet • 802.11 a/b/g/n (WiFi) • 2.5/3G (GPRS, CDMA, EV-DO, EDGE, HSPDA, etc.) • Bluetooth • WiMAX • Infrared • Firewire • Dial-up modems Enable/disable bridging between various network interfaces
Display/UI	• Friendly, easy to use dashboard display • Threat blocking notification • At-a-glance summary on Windows Taskbar
Events	• Configurable event displays • Search and sort capabilities - for events
Wireless Risk Level	• Automatic calculation of wireless risk level • Tutorial help menus, diagnostic tools for decreasing risk • Automatic notification on risk level changes
Automatic Configuration	• Zero user configuration required • Automatic AP addition • Automatic event configuration • Automatic security profile configuration
Automatic Install/Deployment	• Microsoft SMS • Altiris
Security Profile Management	• Enable/disable automatic threat blocking • Define minimum required security behavior • Disable ad-hoc (peer to peer) networking • Disable simultaneous wired/wireless connections • VPN detection
Threat Blocking	• Connection to non-allowed (rogue) AP • Evil twin attacks (AP Phishing) • Connection to SSIDs with multiple MAC addresses • Connection to Hotspot SSID
Server Integration	• Centralized policy management • policy groups • Automatic policy synchronization with scheduling options • Administration of multiple profiles • Current client status • On-demand detailed client report • Audit trail for wireless behavior when out of the office • Automatic client authorization • Shared key authentication of SAFE clients
Client System Requirements	
Processor	Pentium 4 or later
RAM	512 MB or greater
Operating System	Windows XP or later .Net framework 2.0
Server System Specifications	
Required Software	SpectraGuard Enterprise 5.5 or later
Network	
Server Interface	Auto-sensing 10/100/1000 Mbps Ethernet
IP Address Assignment	Static
Environmental	
Operating Temperature	10 to 35° C
Storage Temperature	-40 to 70° C
Humidity	Non-Operating: 95%, non-condensing at 30°C
Power Supply	
Standard Server	Autosensing 100-127/200-240 V, 50/60 Hz, 6/3 A
Premium Server	Autosensing 100-127/200-240 V, 50/60 Hz, 5/2.5 A
Physical Specifications	
Standard Server Dimensions	17 x 26 3/4 x 1 3/4 in (w x d x h), 432 x 680 x 45 mm
Standard Server Weight	24 lbs (10.91 kg)
Premium Server Dimensions	17 x 29 x 1 3/4 in (w x d x h), 432 x 737 x 45 mm
Premium Server Weight	28.9 lbs (12.73 kg)

AirTight® NETWORKS