



Managing Wireless Clients with the Administrator Tool

Intel® PROSet/Wireless Software 10.1



This document is provided "as is" with no warranties whatsoever, including any warranty of merchantability, non-infringement fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification or sample

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel does not control or audit the design or implementation of 3rd party benchmarks or websites referenced in this document. Intel encourages all of its customers to visit the referenced websites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel PROSet/Wireless Software, Intel PRO/Wireless 2200BG Network Connection, Intel PRO/Wireless 2915ABG Network Connection, Intel PRO/Wireless 3945ABG Network Connection, Intel Centrino and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Actual measurement results may vary depending on the specific hardware and software configuration of the computer system measured, the characteristics of those computer components not under direct measurement, variation in processor manufacturing processes, the benchmark utilized, the specific ambient conditions under which the measurement is taken, and other factors.

All plans, features and dates are preliminary and subject to change without notice.

* Third-party brands and names are the property of their respective owners.

Copyright © Intel Corporation 2006



Contents

1	Executive Summary	2
2	Administrator Tool Overview	3
2.1	Key Administrator Tool Features	3
2.1.1	Centralized Client Control	3
2.1.2	Advanced Profile Management	3
2.1.3	Remote Management of Global Policies	4
3	Administrator Tool Test Drive.....	5
3.1	Installing the Administrator Tool.....	5
3.2	Creating an Administrator Package	5
3.2.1	Creating Administrator Profiles.....	6
3.2.2	Configuring Application Settings	9
3.2.3	Configuring Adapter Settings	10
3.2.4	Configuring Software Deployment.....	11
3.2.5	Identifying EAP-FAST A-ID Groups	11
3.3	Deploying Administrator Packages	12
4	Promiscuous Mode	13
5	Conclusion	13



1 Executive Summary

Rapid growth in the corporate deployment of wireless networks has resulted in increased complexity of managing clients to maintain the integrity of the enterprise network. Centralized deployment and management of wireless clients is essential for IT organizations to enforce global policies.

Intel worked with enterprise IT organizations to identify their requirements for effective and efficient wireless client management deployment. The Intel® PROSet/Wireless Administrator Tool directly mirrors the results of these engagements. The Administrator Tool addresses the need for control over wireless clients within the enterprise environment by enabling:

- Remote and local deployment of connection profiles
- Enforcement of corporate network and security policies
- Interaction with current software deployment tools

The Intel® PROSet/Wireless client for Intel® Centrino® mobile technology-based notebooks combined with the Administrator Tool delivers a complete enterprise wireless client management solution.

This white paper presents the key features of the Administrator Tool and how they address today's challenges for IT managers and administrators. It takes the reader on a hands-on test drive of the Administrator Tool to experience its powerful tools for centralized configuration and management of wireless clients.

2 Administrator Tool Overview

The key design goal for the Administrator Tool is empowering IT administrators with the same remote management capabilities for wireless clients as they have for wired clients. The Administrator Tool is designed for manageability, controllability and usability. It eliminates tedious, time consuming, and costly setup of wireless clients. Once clients are set up, the Administrator Tool provides features to ensure ongoing control of clients in today's changing wireless network environment.

The Administrator Tool delivers real cost-saving benefits to enterprises through simplified management, greater control over wireless clients, and increased productivity. It enables IT departments to perform these client management tasks:

- Create customized install packages for easy configuration, management and deployment of wireless clients
- Create user specific, common, Single Sign On (SSO) support with pre-logon and persistent connection profiles to provide advanced, secure wireless connections
- Create packages customized to include configurable application settings, adapter settings, Intel® PROSet/Wireless software components and EAP-FAST A-ID Groups

The blend of innovative design and robust features makes the Administrator Tool the ideal wireless client management choice for any enterprise supporting Intel® Centrino® mobile technology environments that include the Intel® PRO/Wireless 3945ABG Network Connection, Intel® PRO/Wireless 2915ABG Network Connection and Intel® PRO/Wireless 2200BG Network Connection wireless network LAN adapters.

2.1 Key Administrator Tool Features

The Administrator Tool is a comprehensive wireless client management solution that delivers these key features to IT administrators:

- Centralized Client Control
- Advanced Profile Management
- Remote Management of Global Policies

2.1.1 Centralized Client Control

The Administrator Tool's Package Creator enables IT administrators to centrally create and password-protect entire client packages that can include everything wireless clients need for secure connections to the corporate network. Administrator Packages can include advanced connection profiles, customized global policies, enterprise-class security configuration, Intel® PRO/Wireless Network Connection drivers, and custom Intel® PROSet/Wireless Software installs in a single executable application.

2.1.2 Advanced Profile Management

Administrator Profiles created in the Administrator Tool provide advanced profile management options including Single Sign On (SSO) profiles to streamline and enhance network access. SSO profiles consist of Pre-Logon and Persistent connections.



Note: Please refer to Section 3.2.1.1 for more details on Pre-Logon and Persistent connection profiles.



The Administrator Tool supports these new SSO enhancements in the Intel® PROSet/Wireless Software v10.1:

- Additional IEEE 802.1x EAP types.
- Auto Server Certificate Enrollment
- Multiple User/Machine Certificate Authentication
- Novel Network Pre-Logon Connect Support for version 4.90
- Cisco Compatible Extensions* support. The Intel® PRO/Wireless 2200BG Network Connection and Intel® PRO/Wireless 2915ABG Network Connection adapters support Cisco Compatible Extensions v3. The Intel® PRO/Wireless 3945ABG Network Connection supports Cisco Compatible Extensions v4.



Note: 802.1x EAP supports machine and user generated certificates: EAP-TLS, EAP-TTLS, PEAP, and PEAP-GTC OTP.

2.1.3 Remote Management of Global Policies

The Administrator Tool offers IT an unprecedented level of control over client machines with ability to create and change global policy settings.

- Administrators can create a profile to limit connectivity based on location. If manufacturing employees are only allowed to connect to the network when their laptops are on the manufacturing floor and not when they are upstairs in the marketing department, a global policy can be created for these employees that only allow connections to the manufacturing network. Even if the client machine finds another network, it cannot connect to the network.
- Administrators can control the access points that client machines can make connections. A client machine may have the ability to connect to multiple networks via a multi-band 802.11a, b and g combination radio. But if corporate policy requires that certain employees only connect on the 802.11b band, the administrator can remotely send a profile to those employees' machines that only allows them to connect to the desired band.
- Administrators can combine remote management via Persistent Connection with Wake on WLAN (WoWLAN) features (available on the Intel® PRO/Wireless 3945ABG Network Connection only) to maintain complete control of wireless clients. Remote management via Persistent connection enables WLAN connections to be maintained even when no user is logged on. WoWLAN support allows remote wake up of notebooks. Using these features, administrators can continually push critical security and software updates to keep clients in compliance with corporate network policies.



Note: Please check with PC manufacturer on WoWLAN support.

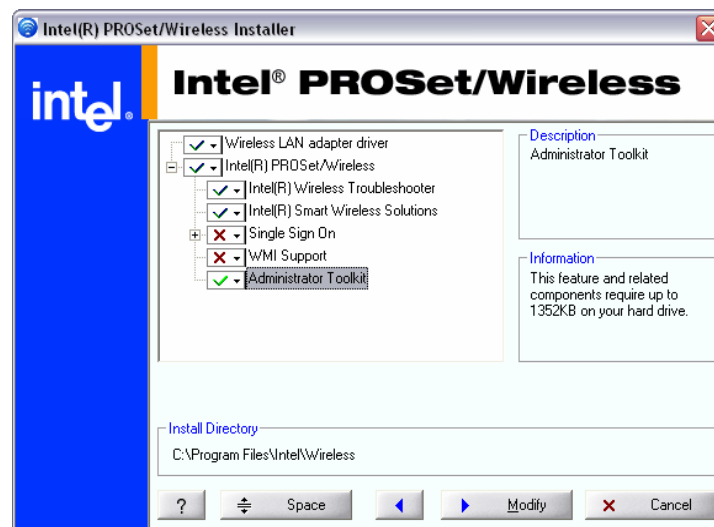
3 Administrator Tool Test Drive

The Administrator Tool's Package Creator enables IT administrators to create complete client packages that can include advanced connection profiles, customized global policies, enterprise-class security configuration, Intel® PRO/Wireless Network Connection drivers, and custom Intel® PROSet/Wireless software installs in a single executable application. The following sections take you on test drive of the Administrator Tool to show the process flow for creating and deploying an Administrator Package.

3.1 Installing the Administrator Tool

The Administrator Tool is an optional software component when installing the Intel® PROSet/Wireless Software. If it is not installed, you need to install it by selecting **Administrator Toolkit** in the Intel (R) PROSet/Wireless Installer (Figure 1). If the Administrator Tool is installed, the **Tools** menu in the Intel (R) PROSet/Wireless window displays the **Administrator Tool** option (Figure 2).

Figure 1: Intel(R) PROSet/Wireless Installer



3.2 Creating an Administrator Package

Selecting **Tools > Administrator Tool** in the Intel(R) PROSet/Wireless window (Figure 2) accesses the Administrator Tool (Figure 4). The first time you launch the Administrator Tool, you are prompted to enter a password. This password prevents unauthorized access to the Administrator Tool. After entering the password, the Open Administrator Package window is displayed for defining a new package or editing an existing package (Figure 3). Select **Create a new package** to define a new package.

The Administrator Tool window organizes client configuration options into five tabbed groups:

- Profiles
- Application Settings
- Adapter Settings
- Software
- EAP-FAST A-ID Groups

To include settings from any of these groups, simply check **Include in this package** at the top of each page and then select the options you want to include in the package. After making all the configuration choices, clicking on the Close button automatically creates the Administrator Package

Figure 2: Launching the Administrator Tool

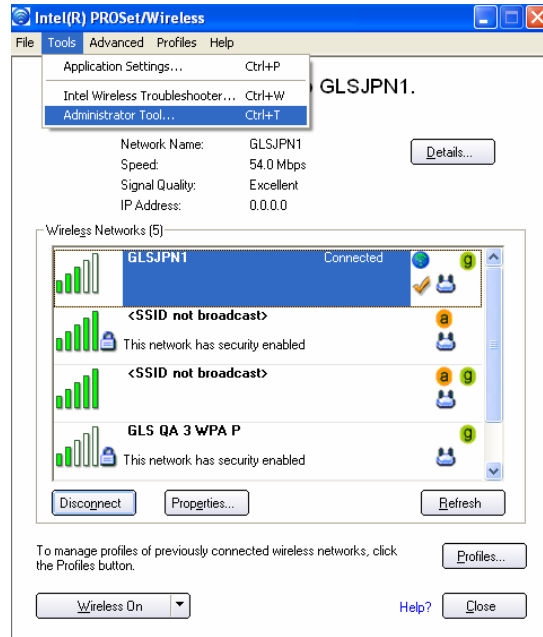
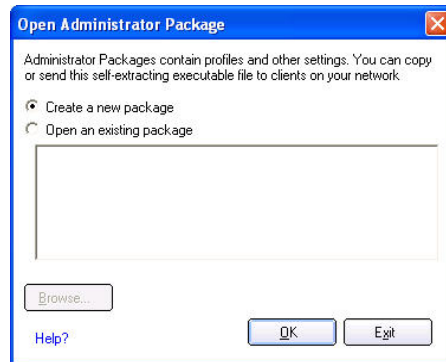
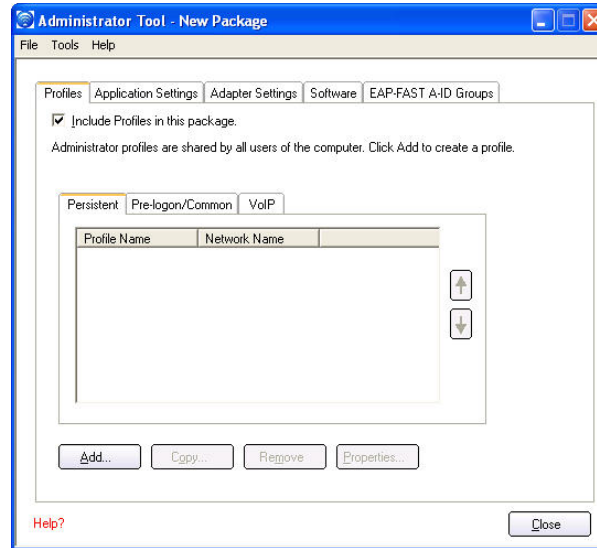


Figure 3: Open Administrator Package



3.2.1 Creating Administrator Profiles

The **Profiles** tab (Figure 4) provides configuration features that enable IT administrators to create advanced Administrator Profiles. These profiles incorporate Single Sign On (SSO) capabilities as well as all the network access and security settings required for wireless clients to access the corporate network. Administrators can create packages that include just Administrator Profiles.

Figure 4: Administrator Tool

3.2.1.1 Pre-Logon and Persistent Connection Profiles

Persistent and Pre-Logon connection features empower IT staff to conduct the same kinds of administrative tasks they do on wired networks with Pre-Logon and Persistent connection profiles.

A Pre-Logon profile is applied and connection is made prior to the Microsoft Windows logon sequence. It allows the IEEE 802.1x credentials to match Microsoft Windows log on user name and password credentials for wireless network connections. The Pre-Logon/Common profile always appears at the top of a Profiles list in the Intel® PROSet/Wireless client. The key benefit of a Pre-Login connection is to enable an administrator to run a login script after domain authentication just like they would in wired networks to enable automatic downloading of critical security patches, operating system patches or anti-virus DAT files.

Persistent connection profiles enable a machine's WLAN connection to be maintained regardless of whether users are logged on or off on the domain and preserves wireless connectivity until the system is powered off. Using a Persistent connection profile, the computer can be managed through the wireless network connection in the same way a computer can be managed on a wired network connection.



Note: Single Sign On (SSO) support must be installed on the wireless client. Pre-Logon support is installed during a Custom install of the Intel® PROSet/Wireless software.

3.2.1.2 Using the Profile Wizard

The Profile Wizard (Figure 5) provides a straightforward method for configuring all the network access and security settings for wireless client profiles. The Profile Wizard includes the following configuration features:

- **General Settings** – Configures wireless network access information (SSID, Pre-Logon and Persistent).
- **Security Settings** – Configures client security settings for the wireless network. Selecting **Enterprise Security** enables IT administrators to configure clients with the latest security industry standards including IEEE 802.11i, IEEE 802.1x, certified Wi-Fi Alliance WPA-Enterprise security, and Cisco Compatible Extensions security enhancements for advanced wireless protection.
- **Advanced** – Clicking the **Advanced** button displays the Advanced Settings window for configuring client global policies. For example, enabling clients to automatically connect to the available network using the profile, specifying a password to restrict network access using the profile.
- **Cisco Options** – Clicking the **Cisco Options** button in the Security Settings page of the Profile Wizard displays the Cisco Compatible Extensions Options window that allows you to take advantage of Cisco WLAN enhancements. The Intel® PROSet/Wireless software v10.1 supports Cisco Light EAP (Cisco LEAP), Cisco Key Integrity Protocol (CKIP), EAP-FAST security features as well as Cisco Rogue Access Point, Fast Roaming using Cisco Centralized Key Management (CCKM), and Mixed-Cell Mode features.



Note: Some features are only compatible with the Intel® PRO/Wireless 3945ABG Network Connection adapter.

Figure 5: Profile Wizard – General Settings

Create Wireless Profile

Profile Name:
General Settings
Security Settings

General Settings

Profile Name:

Wireless Network Name (SSID):

The Profile Name is your name for the network. Example: Home or Office. The Wireless Network Name (SSID) is a unique identifier that differentiates one wireless network from another.

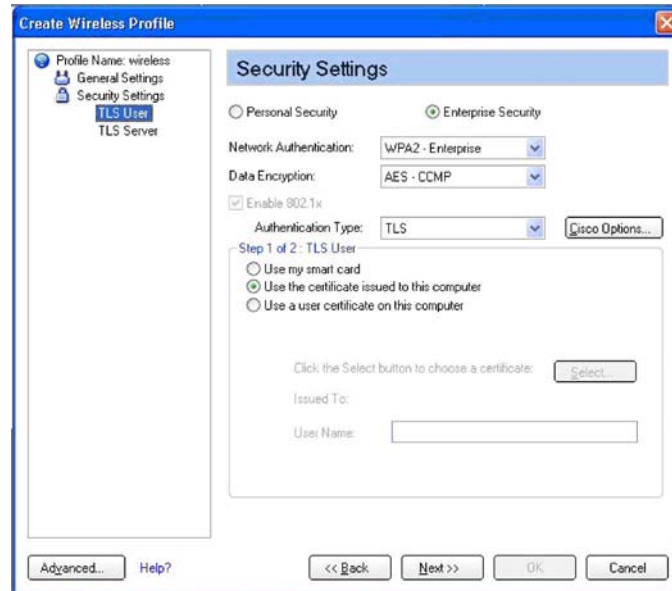
Operating Mode: Network (Infrastructure)

Administrator Profile Type:

Persistent: Active when no users are logged on.

Pre-logon/Common: Active when a user is logged on. This profile is shared by all users.

Advanced... Help? << Back Next >> OK Cancel

Figure 6: Profile Wizard – Security Settings

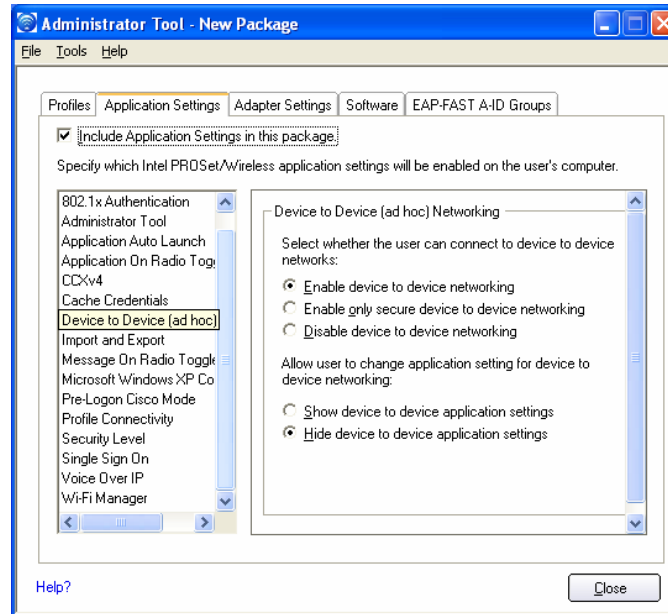
3.2.2 Configuring Application Settings

Features in the **Application Settings** tab (Figure 7) allow the administrator to define how the Intel® PROSet/Wireless client behaves once the package is deployed.

For example, a common corporate policy is not allowing employees to set up or join device-to-device (ad-hoc) wireless networks. Using Application Settings, this feature can be disabled to prevent end users from creating unauthorized device-to-device networks that compromise enterprise information security or leave machines open to unauthorized access.

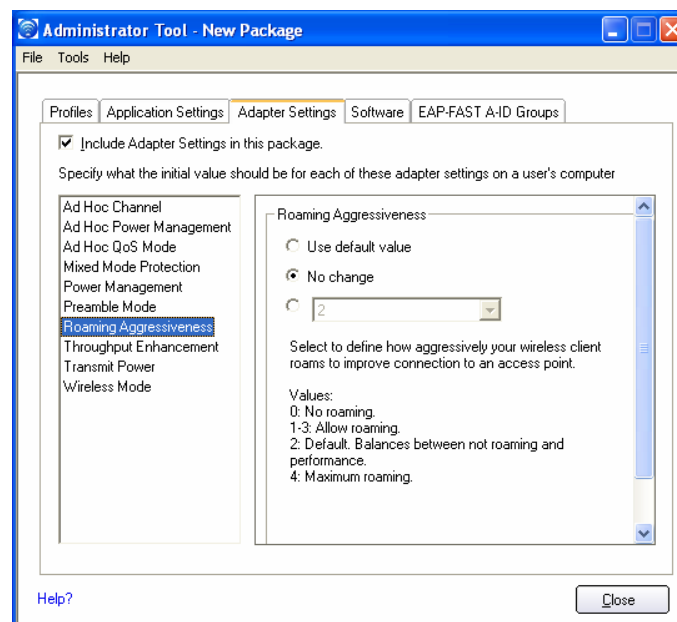
Administrators can also enable client machine with association of a specific program to be started when a wireless connection is made with this profile. For example, this configuration enables users to specify automatic launch of programs such as virtual private network (VPN) or a browser every time upon a user connection to a hotspot – and they can pre-populate the profile for the specific hotspot.

There are additional configuration options available as shown in Figure 7.

Figure 7: Application Settings

3.2.3 Configuring Adapter Settings

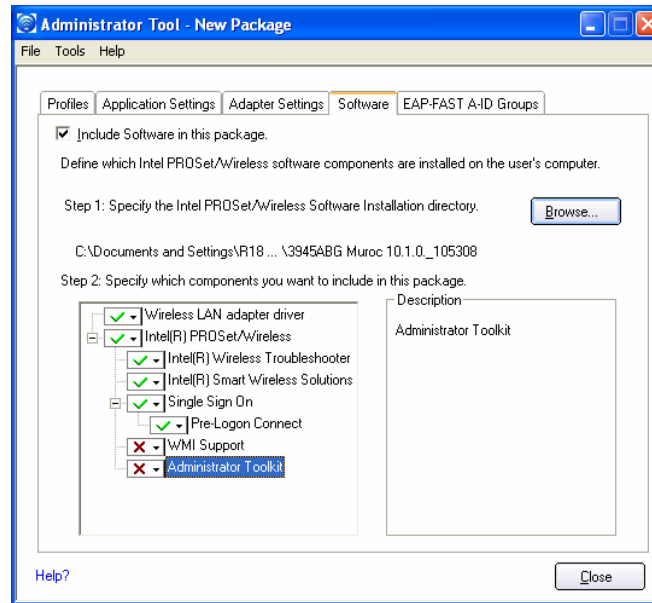
Features in **Adapter Setting** tab (Figure 8) enable the administrator to fully control the adapter settings for the particular network infrastructure deployed. For example, administrators have options to adjust roaming aggressiveness and select values that provide optimal balance between roaming and performance.

Figure 8: Adapter Settings

3.2.4 Configuring Software Deployment

Features in **Software** tab (Figure 9) allow administrators to deploy customized versions of the Intel® PROSet/Wireless software and drivers to remote machines. Because of the modular design of the Intel® PROSet Wireless software, administrators can specify the desired components of the software using the intuitive GUI, rather than the entire solution. This selective install can be done by allowing the user to check off the desired components. This creates a single exe package that can be silently installed on the client systems.

Figure 9: Software

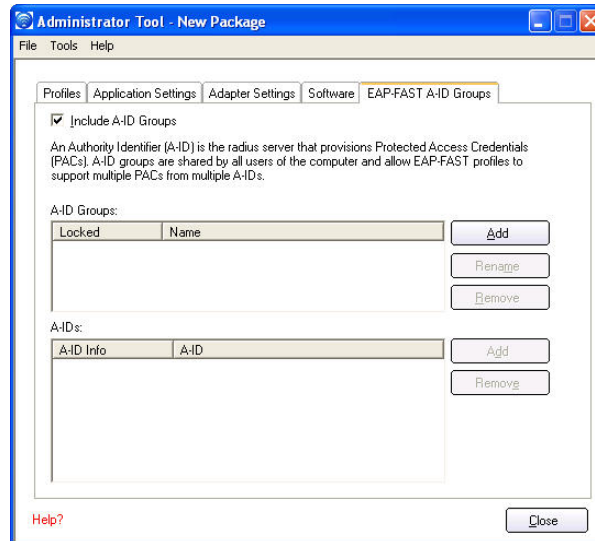


3.2.5 Identifying EAP-FAST A-ID Groups

The **EAP-FAST A-ID Groups** features are available with Cisco Compatible Extensions, which add new support for Voice QoS/Call Admission Control and other related key security enhancements.

An Authority Identifier (A-ID) is the RADIUS server that provisions Protected Access Credential (PACs) A-ID groups. A-ID groups are shared by all users of the computer and allow EAP-FAST profiles to support multiple PACs from multiple A-IDs.

The A-ID groups can be pre-configured by the administrator and set up through an Administrator package on a user's computer. When a wireless network profile encounters a server with an A-ID within the same group, it uses this PAC without a prompt to the user.

Figure 10: EAP-FAST A-ID Groups

Note: For more information on EAP-FAST A-AD Groups please refer to www.cisco.com.

3.3 Deploying Administrator Packages

Once administrators have created and saved Administrator Packages with connection profiles, custom policy settings, and Intel® PROSet/Wireless Software driver and application configurations that meet their company's policies, they can easily save, copy, and export these self-extracting executable packages to clients on their network. When the executable runs on the destination machine, the new configuration is automatically updated. Upon launch of the installed package, the application checks the driver version to assure that a compatible driver is installed. This can be performed by means of a silent install option that requires minimal user intervention.

Administrators can distribute these packages using existing network software distribution tools. For Microsoft users applications like Group Policy Objects (GPO) or Systems Management Server (SMS) enables IT administrators to seamlessly and automatically push the updates to selected group of clients or machines on their network. The .exe file generated with the Administrator Tool can be easily converted by the third party programs to the native .msi file format in order to be pushed out via GPO. Administrator can selectively copy the executable file to any user's computer in order to install the configuration that has been saved in the package. Administrators can also use third-party software distribution packages from LANDesk*, Computer Associates*, and Symantec* etc., to distribute these packages or less advanced distribution mechanisms such as e-mail or posting exe files on the intranet server to deploy these packages.

Once an Administrator Package is installed on the Intel® PROSet/Wireless client, the new Administrator Package is automatically installed. The top-priority placement of the connection profile ensures the client complies with global network and security policies whenever connecting to the enterprise environment. The user cannot re-prioritize, modify or remove this profile.



4 Promiscuous Mode

Intel® PROSet/Wireless Software v10.5 supports new feature called promiscuous mode. In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. Sniffers operate with the network card/driver in this mode to be able to capture all packets. Packets can be captured and saved for analysis in order to monitor network usage or activity.

Independent Software Vendor (ISV) applications and the operating system (OS) use promiscuous mode to monitor Wireless LAN network performance. Promiscuous mode allows a network adapter to capture and read layer 2 packets, IEEE 802.11 data, management, control, and error frames. It also includes unicast, multicast, and broadcast packets. The captured packets can be passed up to an application for network monitoring and analysis. Microsoft Windows 2000* and Microsoft Windows XP*, Intel® PROSet/Wireless Software v10.5 supports ISV promiscuous mode, i.e. support for ISV sniffer application operating on top of Intel® PRO/Wireless 3945ABG Network Connection adapter.

The ISV promiscuous mode is currently supported by AirMagnet* sniffer.

Note: This feature is not enabled with the Intel® PRO/Wireless 2200BG and Intel® PRO/Wireless 2915ABG Network Connection hardware.

5 Conclusion

The Administrator Tool incorporates a powerhouse of innovative features to empower administrators with greater freedom and level of control over their wireless clients. These features allow safe adoption of cutting-edge wireless technology to achieve competitive market advantage, lower total cost of ownership (TCO) for wireless deployments, enable full compliance with corporate network and security policies, make wireless computing seamless for employees to maximize productivity, and dramatically reduce costly IT support calls.