



AirWave Management Client™ Installation & User Guide

Version 4.3

Copyright © 2006 AirWave Wireless, Inc. All rights reserved. This document contains confidential and proprietary information, and is intended for licensed users only. Any unauthorized copying, distribution, or disclosure of information is a violation of copyright laws and is strictly prohibited.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of AirWave Wireless, Inc.

Table of Contents

Introduction	3
System Requirements	3
Functional Overview	4
Configuring AMP	5
Downloading the AirWave Management Client	5
Installing the AirWave Management Client	5
Initiating the AirWave Management Client	8
Using the AirWave Management Client	10
Recommendations for Deploying the AirWave Management Client	13
Troubleshooting and Uninstalling the AirWave Management Client	14
AMC Diagnostics Procedures	15
Common Questions	18
Appendix A: Pinging AMP from AMC	19
Appendix B: Reference HTML Post	20
Appendix C: Configure MS Personal Firewall - AMC to AMP Communication	22
Appendix D: View AMC Log File	23

Introduction

The AirWave Management Client™ (AMC) is a software utility that enables client devices to act as passive RF “sensors” and to communicate directly with the AirWave Management Platform™ (AMP) wireless network management software. When used in conjunction with AMP, the AirWave Management Client can dramatically improve both wireless network security and performance:

Enhance rogue AP detection	<i>Every AMC-enabled client device becomes an additional RF “sensor” that scans for unauthorized wireless access points within range, greatly increasing the chances that a rogue device will be discovered.</i>
Improve RF monitoring	<i>Each AMC-enabled client reports up-to-date information about the RF environment to AMP. AMP correlates this data with other information to diagnose RF interference and other common RF problems</i>
Help users avoid rogue APs and ‘man-in-the-middle’ attacks	<i>AMC displays a list of all APs in range and alerts users when they are connected to an unknown, unmanaged access point. With AMC, users can ensure that they associate only to secure, managed devices.</i>
Minimize RF interference	<i>AMC helps determine which access points are within RF range of one another, enabling network administrators to set these neighboring APs to non-overlapping channels to minimize RF interference</i>
Balance network load	<i>AMC tells users which access points are being over-used, helping them quickly select APs with greater bandwidth availability in crowded high-usage environments.</i>

AMC version 1.1 supports Microsoft Windows XP devices. Future product releases will support other devices and operating systems. Contact your AirWave Territory Sales Manager or 866-802-1121 for additional information.

System Requirements

AirWave Management Platform™

- AMP v3.0 or higher
- AMP’s IP address or Hostname
- AMP “client” user password

Minimum Client Requirements

- Intel Pentium 4 processor (or equivalent)
- Microsoft Windows XP with SP1
- 11 Megabytes of disk space
 - 3 MB application files
 - Log file can grow to a maximum of 4 MB, with additional space for log backups

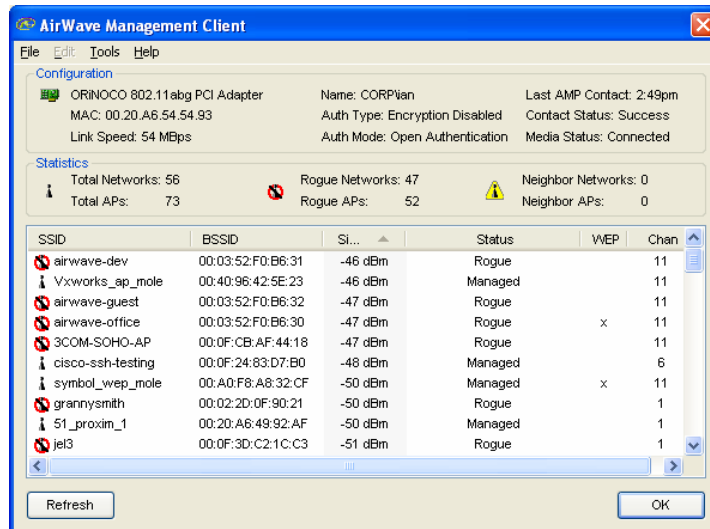
Functional Overview

The AirWave Management Client is a very lightweight and completely passive application that utilizes Microsoft's NDIS layer and is fully compatible with all 802.11 client cards with NDIS 5.1 certification.

1. Once installed on the client device, AMC runs in the background to collect statistics from NDIS on all other RF devices within range (including BSSID, SSID, WEP Bit, Channel, Signal Strength, and Device Mode). AMC polls NDIS every five minutes when minimized and once per minute when maximized.
2. AMC securely posts the list of detected RF devices to the AirWave Management Platform via HTTPS and waits for AMP to respond with additional information about these devices.
3. AMP analyzes the list of devices discovered by AMC and compares the Radio MAC (BSSID) of these devices to AMP's list of managed access points:
 - a. If the Radio MAC of a discovered device is associated with an access point that is already under management by AMP, AMP simply records the new RF data.
 - b. If the Radio MAC of a discovered device is associated with a previously detected rogue access point, AMP updates its records to reflect the AMC client as an additional Discovering Agent and generates a Rogue AP alert.
 - c. If the Radio MAC of a discovered device is not previously known and managed by AMP, AMP automatically generates a Rogue AP alert and records the AMC client as the "Discovering Agent."
4. Once AMP has analyzed the list of discovered devices, it sends AMC a 'Return List' with additional data about those devices, including: BSSID, AMP Status and AP Load.

AP Load (*Heavy, Medium, or Low*) – An overall AP utilization metric, based on number of users, bandwidth utilization, error counters, etc., that provides a real-world load indicator.

AMP Status (*Managed, Rogue, Neighbor*) – Indicates whether the discovered devices is an authorized access point ("Managed"), a potential rogue access point ("Rogue") or a known AP that is not being managed by the organization's network administrators, such as an AP installed in a neighbor's offices ("Neighbor").

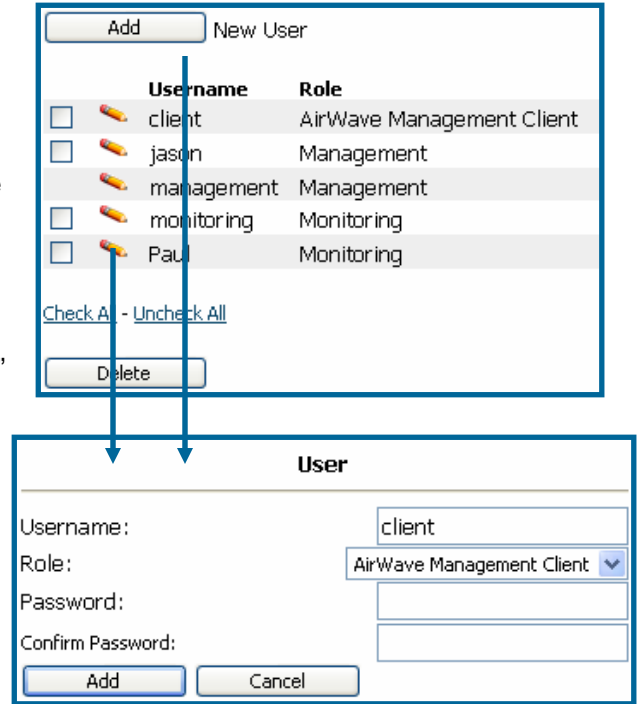


- Once AMC receives the Return List from AMP, it combines this information with what is already known and displays an updated list of APs within range. The combined set of information includes SSID, Radio MAC, WEP Bit, Channel, Signal Strength, Device Mode, AMP Status, and AP Load.

Configuring AMP

- Browse to the **AMP SETUP→Users** page on AMP's web UI.
- Ensure there is a "client" user assigned to the "AirWave Management Client" role.
- If a "client" user does not exist:
 - Click "Add" button.
 - Enter "client" as Username.
 - Assign "AirWave Management Client" role.
 - Enter password.
 - Click "Add" button to save.
- To change "client" user's password:
 - Click on the pencil icon next to client row.
 - Enter new password.
 - Click "Add" button to save.

NOTE: The AMC password must correspond with this password in order to establish communication between AMP and the AirWave Management Client.



Downloading the AirWave Management Client

If you have an AMC install CD proceed to the "Installing the AirWave Management Client" section.

- The AirWave Management Client setup utility can be downloaded from AirWave's website at <http://www.airwave.com/install/AMCSetup.msi>. You will be prompted to provide a username and password. *To obtain the password, please contact AirWave Technical Support at support@airwave.com or 866-943-4267 (866-WIFI-AMP).*
- Save the AMCSetup.msi file on your machine or to a network server for future distribution.

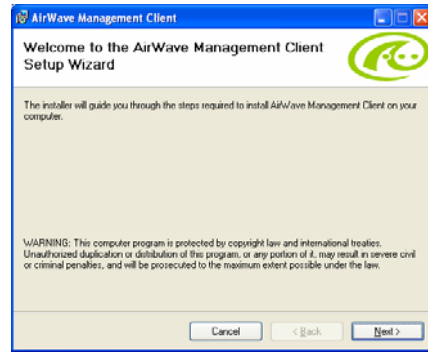
OR

- Download the AMC setup utility from the Rapids page on any AMP version 3.1.2 or later.

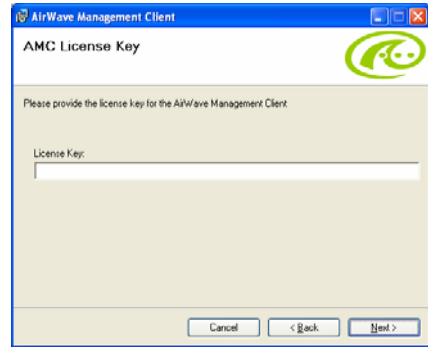
Installing the AirWave Management Client

- If you are installing off of the AMC Install CD, autorun may automatically launch the AirWave Management Client Setup Wizard. If autorun is disabled, or if you downloaded the setup utility from AirWave's web site, double-click the setup file AMCSetup.msi from the CD-ROM folder or from the folder into which you saved the downloaded file.

2. When the AirWave Management Client Setup Wizard appears, click "Next" to proceed with the installation or click "Cancel" to exit.

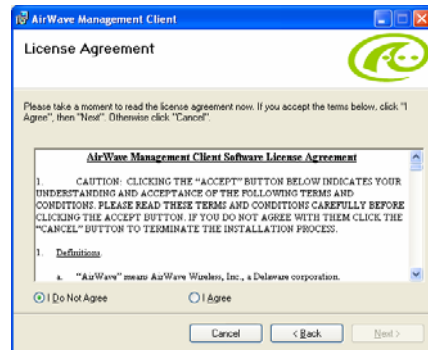


3. Enter the license key for your AMC installation. Once entered, click "Next" to proceed with the installation or click "Cancel" to exit.

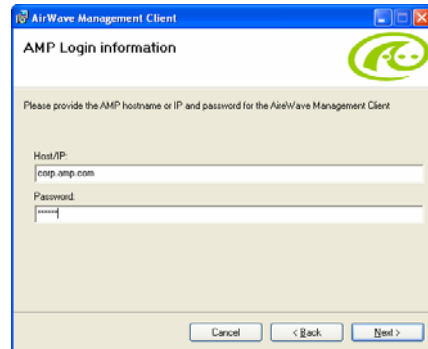


4. Read the AirWave Management Software License Agreement. Click "I Agree" and "Next" to proceed, "Back" to return to the Welcome Screen, or "Cancel" to exit.

Please read the license agreement in its entirety prior to agreeing with the terms.



5. To enable communication between AMC and the AirWave Management Platform, enter AMP's Host Name/IP and the "client" password (see the "Configuring AMP" section above). Click "Next" to proceed, "Back" to return to the License Agreement, or "Cancel" to exit.

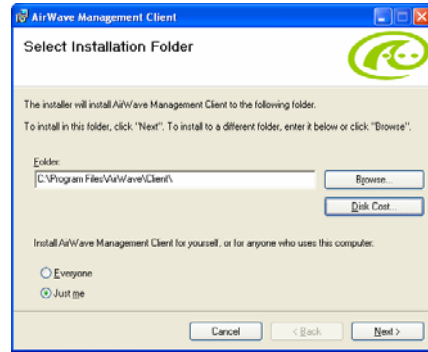


6. Select the installation folder for the AirWave Management Client. After selecting the installation folder click “Next” to proceed or “Cancel” to exit.

Note: The default installation target conforms to Microsoft’s recommendation

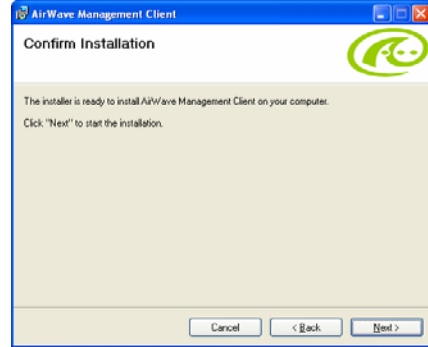
- a. Click the “Disk Cost” button to ensure you have sufficient disk space available to install AMC.
- b. Use the “Everyone/Just Me” toggle to determine whether other users of your computer should be allowed to run AMC.

7. When the Confirmation window, appears click “Next” to start the installation.



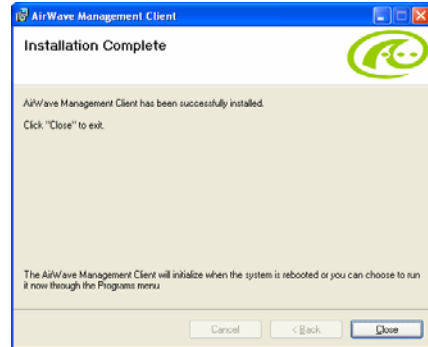
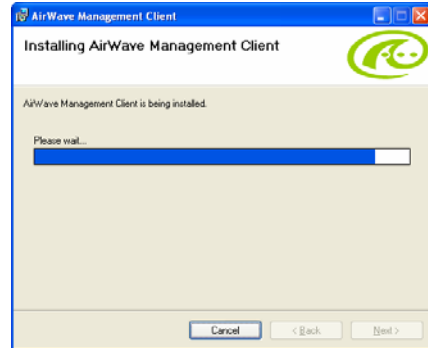
8. AMC Setup Wizard will display the progress of the installation process.

Note: The installation should complete in less than 1 minute.



9. When the “Installation Complete” window appears, click “Close” to exit the AMC Setup Wizard.

Note: AMC will not launch automatically upon installation.



Initiating the AirWave Management Client

The AirWave Management Client automatically runs upon startup, minimized in the task tray to be unobtrusive and utilize minimal system resources.

- To initiate AMC, you may:
 - Reboot your computer to automatically initiate AMC.

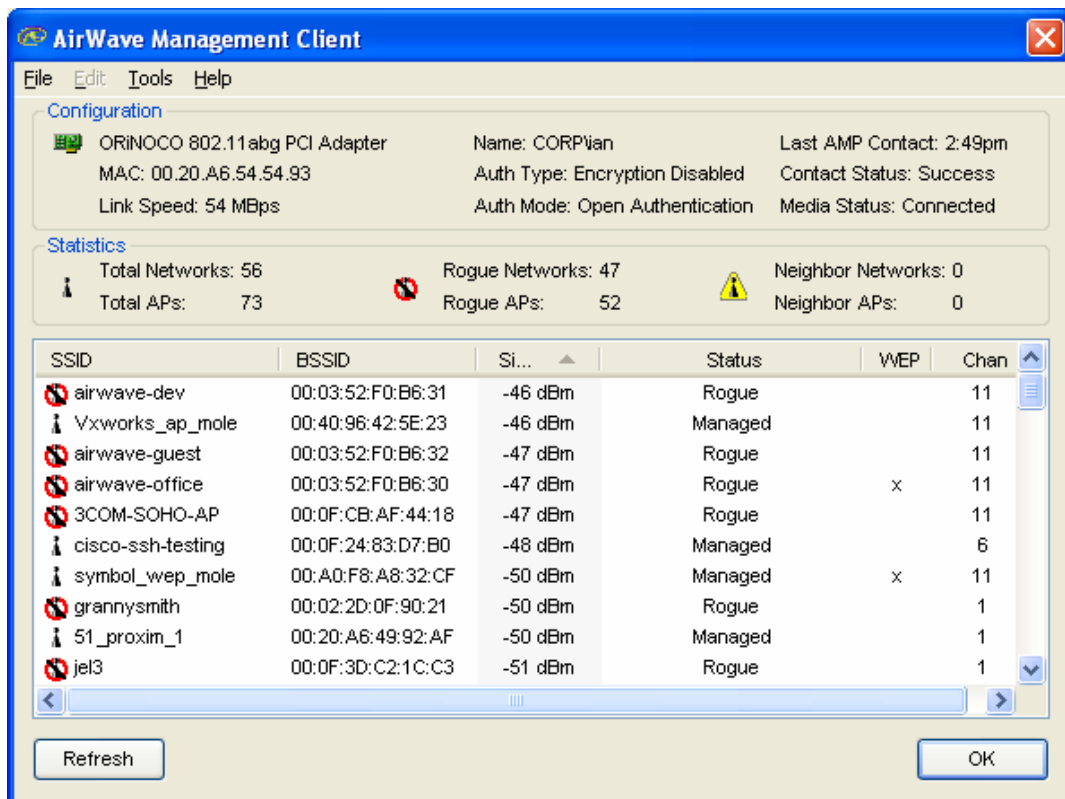
OR

 - Execute "C:\Program Files\airwave\AirWave Management Client\AMClient.exe" from the command line or Windows Explorer.
 - Click the AirWave icon on **Start→All Programs**.

OR

 - Complete the install and allow the default settings to launch the AMC.

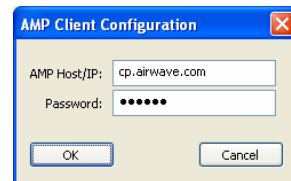
- Once initiated, AMC will remain minimized as the AirWave icon in the task tray.



- To maximize AMC, double-click the AirWave icon in the task tray.
- The maximized AMC displays:

Field	Notes
Configuration Section	
Card	<i>Radio manufacturer and model</i>
MAC	<i>MAC address of the client computer</i>
Link Speed	<i>Current link speed connection of the client computer</i>
Name	<i>Domain user name</i>
Auth Type	<i>Wireless authentication type</i>
Auth Mode	<i>Wireless authentication mode</i>
Last AMP Contact	<i>Last time AMC initiated communications with AMP</i>
Contact Status	<i>Status of the last AMC communication with AMP</i>
Media Status	<i>Status of the network connection</i>
Statistics Section	
Total Networks	<i>Total number of SSIDs observed by the client computer</i>
Total APs	<i>Total number of APs observed by the client computer</i>
Rogue Networks	<i>Total number of "rogue" SSIDs observed by the client computer.</i>
Rogue APs	<i>Total number of rogue APs observed by the client computer</i>
Neighbor Networks	<i>Total number of SSIDs observed by client computer that are in "ignored" state on AMP</i>
Neighbor APs	<i>Total number of APs observed by client computer that are in "ignored" state on AMP</i>

- To minimize AMC, select **File→Close** or click the X in the top right corner. Although the program window closes, AMC will continue to run in the taskbar and will continue gathering and reporting RF statistical information.



- To configure communication with the AirWave Management Platform, select **Tools→Configure**. Enter the AMP Host/IP and password information for the "Client" user in the popup window.
- Select **H**elp to access online help.




Using the AirWave Management Client

1. Identifying and avoiding rogue access points from the client device:

- a. Any unknown, unmanaged networks within range are marked as rogues on AMC's interface with a red circle and the word 'Rogue.' Wi-Fi users should be instructed not to associate to networks marked as rogues.

2. Detecting man-in-the-middle attacks from the client device:




- a. Click on the "SSID" column to sort by SSID.
- b. Locate the SSID with the blue circle, indicating the network to which the client computer is currently associated.
- c. Determine if there are rogue APs within range of the client that are broadcasting

	airwave-dev	00:03:52:F0:B6:34	1	-39 dBm		Rogue
	airwave-eap	00:40:96:40:0B:7C	11	-58 dBm	x	Rogue
	airwave-eap	00:09:B7:F4:E7:99	6	-73 dBm	x	Managed





with the same SSID of the authorized access point. In the example above, there are two access points broadcasting with SSID of "airwave-eap". One of them is a known, managed access point (00:09:B7:F4:E7:99). The other access point (00:40:96:40:0B:7C) is an unknown, unauthorized rogue access point that has been configured with a legitimate SSID in an attempt to get users to unwittingly connect to it.

3. Using AMC to monitor the RF impact of neighboring access points

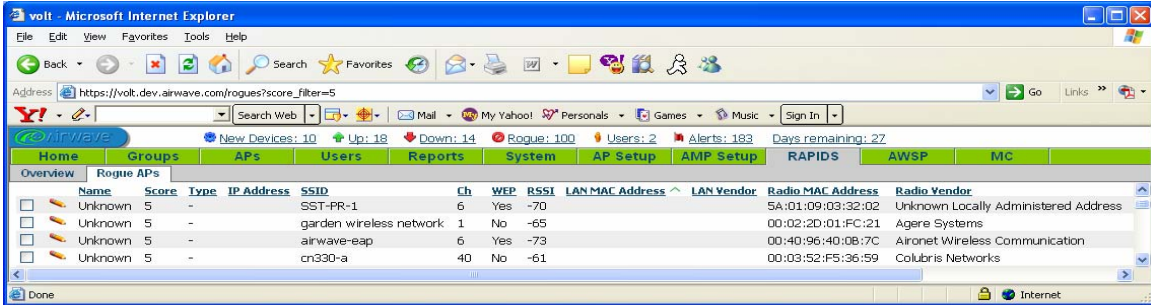
- a. Note the channel and Signal Strength of each access point. In this example, the access point to which the client device is connected is set to channel 6 and the current signal strength is "-73 dBm".

	airwave-dev	00:03:52:F0:B6:34	1	-39 dBm		Rogue
	airwave-eap	00:40:96:40:0B:7C	11	-58 dBm	x	Rogue
	airwave-eap	00:09:B7:F4:E7:99	6	-73 dBm	x	Managed

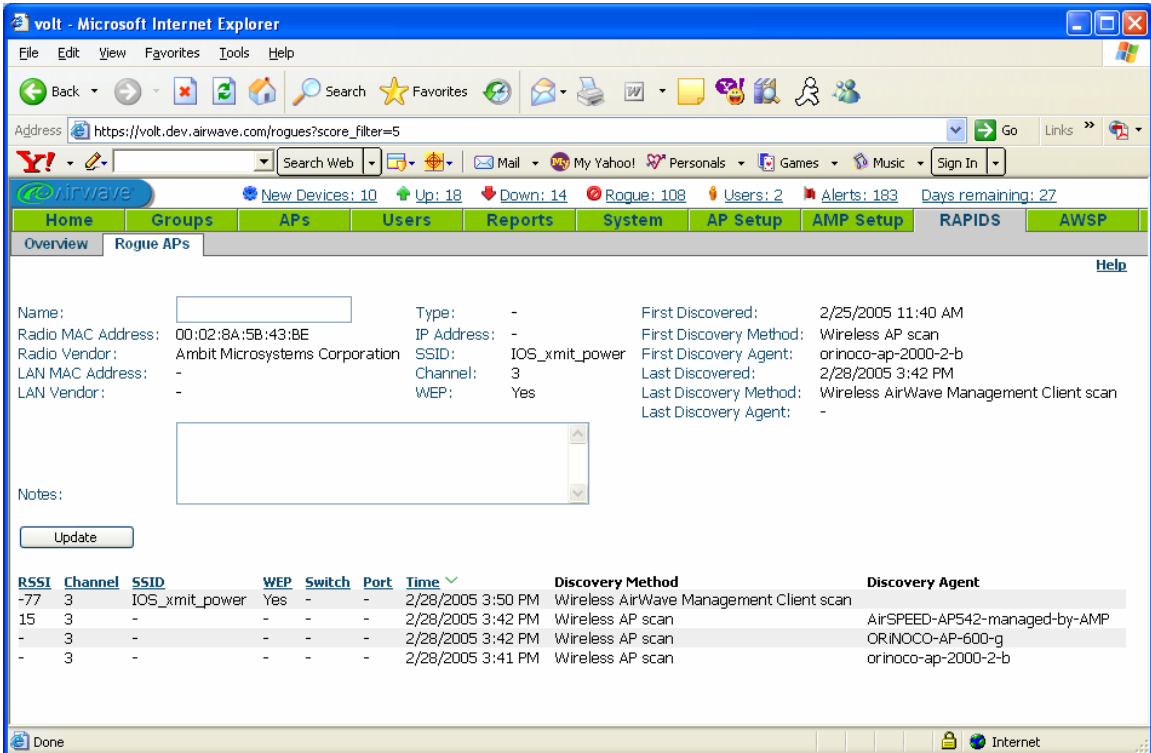
- b. Click the "Channel" heading to sort the list of APs by channel.
- c. Determine if other access points within range are transmitting on the same channel. If there are other APs transmitting on this channel, determine which of these APs has the strongest overlapping signal. In this example, several access points are transmitting on channel 6, but the two APs creating the most interference for the client are the access points with the highest observed signal strength: the APs with Radio MACs of "00:0E:38:62:61:20" and "00:02:2D:3A:09:A9". (NOTE: Signal strength data is a negative number, so -58 dBm indicates a stronger signal than -87 dBm).

	airwave-eap	00:09:B7:F4:E7:99	6	-58 dBm	x	Managed
	hp420-ohm-bbb	00:0D:9D:C6:78:C5	6	-87 dBm	x	Managed
	Wireless Network	00:0E:38:62:61:20	6	-72 dBm		Managed
	medical	00:02:2D:3A:09:A9	6	-72 dBm		Rogue

4. **Using AMC to ensure that the user is connected to the AP with the strongest RF signal.**
 - a. Sort the list of APs by SSID by clicking on the “SSID” column heading.
 - b. Locate the network to which the user is currently associated (the blue circle icon).
 - c. If other managed APs are available, analyze their signal strength and determine whether any of them would provide a stronger signal.
5. **Using AMC and the AirWave Management Platform™ to automatically detect rogue APs**
 - a. Whenever a client with AMC software detects a rogue access point within range, AMP automatically generates an alert and adds that device to the list of suspected rogues. To see the complete list of rogue APs via AMP’s web-based user interface, Click on the “Rogues” link at the top of the management page.



- b. On the **APs→Rogue** page, select the rogue device that you would like to investigate by clicking the link associated with the “Name” of the device (in this example, “Rogue Airport (RG-1000)” is the device to be investigated).
- c. AMP then displays all current and historical data related to the selected rogue device:



- In this case, the AirWave Management Platform has detected this rogue access point via three different methods:
 - *RF scanning via an AMC-enabled client* device with MAC address 00:90:4B:64:CE:23 (AMP displays the MAC address of the client device in the “Discovering Agent” column).
 - *RF scanning via managed access points* named “office-ap1” and “office-ap2”.
 - *Wireline detection* via an SNMP scan of the network that identified this as a potential rogue device.
- RSSI values from wireless scans may be used to roughly triangulate the physical location of the rogue access point. This rogue device is within RF range of office-ap1, office-ap2, and the AMC-enabled client. The strength of the signal detected by the AMC-enabled client is weak, indicating that the rogue may be relatively far away. *NOTE: RSSI values reported by access points may vary from manufacturer to manufacturer, so RSSI often provides only a rough indication of the location of the AP.*

Recommendations for Deploying the AirWave Management Client

The best candidate systems for AMC are stationary desktop computers. The best way to triangulate a Rogue access point is by utilizing fixed points of reference. If the desktop computer is not equipped with wireless NICs, a combination 802.11a/b/g wireless client card is recommended. An 802.11a/b/g wireless card can scan 2.4 GHz and 5 GHz providing the greatest level of protection. USB wireless client adapters are recommended for their ease of installation, because they don't require opening the computer.

After installing the wireless card, disable all protocols associated with the wireless NIC (Client for Microsoft Networks, File and Print Sharing Microsoft Networks, QoS Packet Scheduler, AEGIS Protocol, and **Internet Protocol (TCP/IP)**). Disabling all protocols will ensure security on the desktop computer; AMC communicates with AMP over the wire.

Utilizing AMC with Laptops can be useful for the final detection step; by watching the Signal Strength Column in AMC you can easily determine when moving closer to the Rogue in question.

Deployments with Legacy APs

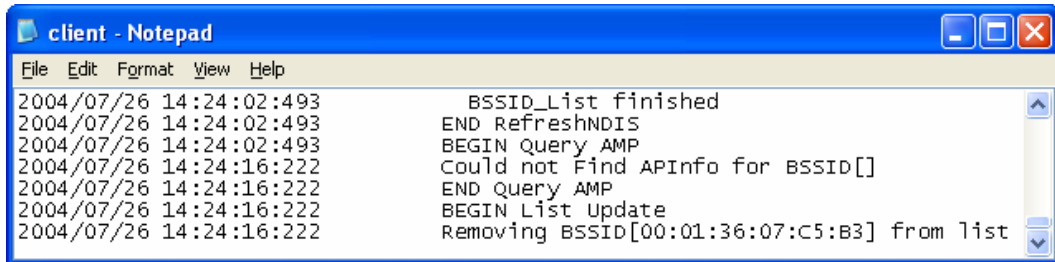
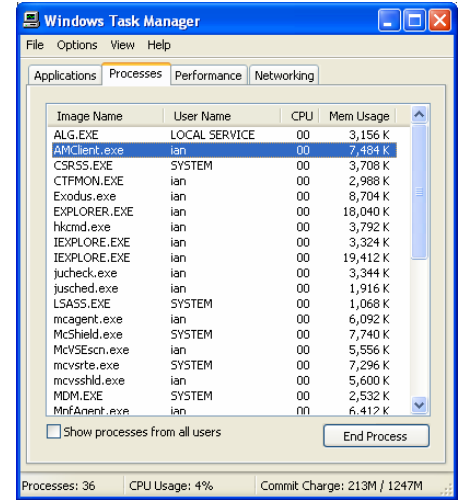
When deploying AMC within legacy WLAN deployments strive to provide full AMC coverage, because legacy access points do not provide the ability to scan for Rogues. These access points include: Artem ComPoint, Avaya AP1 and 2, Cisco VxWorks 340, 350, and 1200, Compaq WL-400, 410, and 510, Enterasys R2, 2000, and 3000, HP 420, IBM AP-500, Nomadix HSG, Proxim/Orinoco 500, 1000, and WavePoint II, Symbol 4121, and Toshiba AP-500. In these environments you should select a grid of desktop PCs each with an estimated 75 foot radius.

Deployments with Scanning APs

In deployments where access point can scan for Rogue access points, AMC should be used to fill in RF coverage holes. Strategically deploy AMC clients near the edges of your building to ensure you get external coverage for hackers located in the parking lot or access points from nearby buildings or businesses. Neighboring access points cause problems without being used by hackers, by causing RF interference that reduces the overall performance of your wireless LAN.

Troubleshooting and Uninstalling the AirWave Management Client

1. To ensure AMC is running and verify memory usage:
 - a. Right-click the Windows task tray and select “Task Manager”.
 - b. Select the “Processes” tab.
 - c. Sort by “Image Name” and search for “AMClient.exe”. In this example “AMClient.exe” is utilizing 7,484 kilobytes of memory.
2. To prevent AMC from automatically running on startup:
 - a. Navigate to Windows **Start→Run** and enter “msconfig”.
 - b. Select the “Startup” tab on the window that is displayed.
 - c. Locate “AMClient” and deselect the “Startup Item” checkbox.
 - d. Click “Apply.”
3. Check AMC log file for errors and status.
 - a. From the command line type: “notepad c:\Documents and Settings\All Users\Application Data\Airwave\AMClient.log”.
 - b. If navigating to this directory in Explorer, note that the Application Data folder is hidden by default in Windows XP.
 - c. Navigate to the bottom of the page, noting any error statements.



4. Check the AMP Event Log file
 - a. To see AMP’s event log, navigate to AMP’s **System→Event Log** page.
5. To uninstall AMC, navigate to Windows **Start→Control Panel→Add or Remove Programs** and locate “AirWave Management Client.” Select “Remove”.

AMC Diagnostics Procedures

If you receive “Failure” status in the Contact Status field on the AirWave Management Client (AMC) use the following steps to diagnose the problem.

Steps 1 and 2 address communication issues between the wireless station and AMP.

1. Ensure ICMP between the wireless station and AMP – see Appendix A Ping AMP for instructions.

Success – Proceed to step #2

- *Wireless Station has ICMP access to AMP.*

Failure

- a. Check security restrictions of access to AMP for user networks.
- b. Ensure AMP’s Hostname/IP are correct.
- c. Ensure the wireless client computer has connectivity and a valid IP.

2. Ensure HTTPS access from the wireless client computer to AMP.

- Point the wireless client computer's browser to AMP's URL.
- You should see the basic auth page.

Success – Proceed to step #3

- *Wireless Station has ICMP access to AMP.*
- *Wireless Station has HTTPS access to AMP.*

Failure

- a. Check the firewall restrictions between the wireless client computer and AMP.



Steps 3 and 4 address the “client” user’s credentials on AMP.

3. Ensure AMP has a “client” user with the proper role, and password.

- Authenticate as any user with a “management” role.
- Navigate to **AMP Setup→Users** page and ensure there is a user named “client, if not create one. The user must be named “client”.
- Ensure the user named “client” has the “AirWave Management Client” role.
- Enter a password for the user named “client” in AMP.

Success – Proceed to step #4

- *Wireless Station has ICMP access to AMP.*
- *Wireless Station has HTTPS access to AMP.*
- *AMP has a "client" user with proper role and password.*

Failure

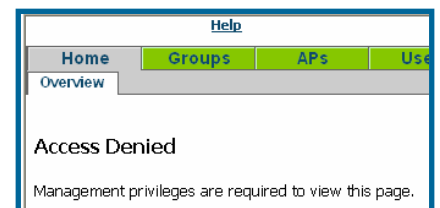
- a. Acquire a “user” with management credentials.

4. Ensure the “client” user credentials are correct.

- Close the browser from step #3 to ensure the credentials are not cached.
- Point a new browser to AMP’s URL.
- When presented with the basic credentials type “client” for the username and the password entered in Step #3.
- You should see “Access Denied”, because the “client” user should not be able to access this page. We are ensuring that the “client” user’s password is correct. If you do not see the “Access Denied” page then you are using the wrong credentials.

Success – Proceed to step #5

- *Wireless Station has ICMP access to AMP.*



- *Wireless Station has HTTPS access to AMP.*
- *AMP has a "client" user with proper role and password.*
- *AMP's "client" user has been validated.*

Failure

- a. Ensure the password entered matches the one configured in step #3.

Step 5 addresses AMC's communication and credential configuration.

5. Ensure the AMC's Hostname/IP is correct.

- On the AMC client proceed to Tools→Configure.
- Ensure AMP's Hostname/IP is correct.
- Ensure the password on the client matches the one entered on AMP in Step #3.

Success – Proceed to step #6

- *Wireless Station has ICMP access to AMP.*
- *Wireless Station has HTTPS access to AMP.*
- *AMP has a "client" user with proper role and password.*
- *AMP's "client" user has been validated.*
- *AMC's Hostname/IP and Password match AMP's.*

Failure

- a. No way to test failure on this procedure.

Step 6 addresses AMP's Client Handler and "client" user credentials

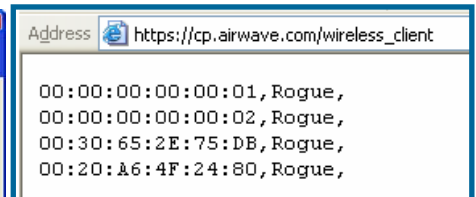
6. Execute the simulated client post listed in Appendix B to determine if the client user and credentials are correct.

- Execute notepad by navigating to Start -> Run and entering "notepad" in the prompt box followed by <RETURN>.
- Cut the text in Appendix B and paste it into notepad.
- Modify the string "cp.airwave.com" to the hostname or IP of the AMP server at your location.
- Within notepad navigate to File->Save As and type in "Clientpost.html" as the filename.
- Launch a new IE window (to alleviate caching problems) and open "Clientpost.html".
- You should see the following screen:

MAC Address	Wireless IP of Client	User Name	Domain Name	Card Manufacturer and Client Firmware
00:00:01:00:00:01	xxx.xx			
00:00:00:00:00:01	foo	1	foo1	0
00:00:00:00:00:02	bar	5	bar1	0
00:30:65:2E:75:DB	dev	11	0	1
00:20:A6:4F:24:80		140	pieces	0

Submit Query

- Click the "Submit Query" button.
- You should see the "Basic Auth Screen".
 - Ensure you are connecting to proper server.
 - Ensure username and password are correct.



- If successful you will see the following results:
Note: There could be browser caching issues.

Success – Proceed to step 7

- *Wireless Station has ICMP access to AMP.*
- *Wireless Station has HTTPS access to AMP.*
- *AMP has a "client" user with proper role and password.*
- *AMP's "client" user has been validated.*
- *AMC's Hostname/IP and Password match AMP's.*
- *AMP's AMC handler is working correctly.*
- *"client" user access level is configured properly.*

Failure

- a. Ensure AMC's password matches the "client" user's password on AMP.

Step 7 addresses AMC application connectivity to AMP.

7. If the previous 6 steps succeed, then there is most likely a personal firewall configuration issue. Although AMC is launching the IE authentication libraries Personal Firewalls are looking at port utilization by application. Most firewalls are configured to block all non-standard applications pushing information from your PC.

Note personal firewall may not always notify you that they are blocking the application.

Success – You should see "Success" in the Contact Status field.

Failure – See documentation

- a. Read personal firewall documentation.
- b. See Appendix D – Viewing Client log file.

Common Questions

Question – Why does another AMC device show more access points?

Answers:

- Your card might be a 802.11b only card and the other user has an a/b/g card.
- Each card's receive sensitivity might be different, some cards are better than others.
- AMC consumes data from the wireless NIC. These cards are doing very fast off-channel (data delivery) scanning, so the card might not report the same APs on each scan.

Question – Why does another AMC show the same Rogue AP on another channel?

Answers:

- AMC consumes data from the wireless NIC. These cards are doing very fast off-channel (data delivery) scanning, so the card might pickup the AP on channel 5 when in reality its channel is configured to 6.
- Each card's receive sensitivity might be different, some cards are better than others

Question – How can I find a Rogue AP once the AMC has discovered it?

Answers:

- Utilize AMP to determine if multiple clients and/or APs have discovered the Rogue AP. If so triangulate based on Signal Strength.
- Move the AMC every minute (that is the maximized refresh rate) and when the signal strength increases (-82 ... -78 ... -60) you are moving in the right direction.

Question – How does the AMC determine if the AP is Rogue?

Answers:

- AMC sends all BSSIDs (APs) in its air space to AMP. AMP determines the status of the AP by checking to see if the Radio MAC exists in AMP's database. If the radio MAC reported by AMC is not managed by AMP (not found as a LAN or Radio MAC), AMP sends back a Rogue status to AMC.

Question – Do I need special drivers or network adapter to utilize AMC?

Answers:

- No. AMC utilizes MS NIDS 5.1 which is supported by all NICs released for Windows XP in the last 3 years.

Question – There are strange MAC addresses beginning with "00:00:00 ..." in my AMC.

Answers:

- This is an Ad-hoc client trying to build an Ad-hoc network.

Question – Will AMC report Rogues when I am in Starbucks?

Answers:

- Yes, if the client running AMC can connect to AMP from Starbucks. You should be very careful with VPNs.

Question – Does AMC start automatically?

Answers:

- Yes, during installation AMC is configured to run on startup. If you wish to disable this feature launch "msconfig" and disable AMClient as a startup item.

Appendix A: Pinging AMP from AMC

Pinging amp.airwave.com [100.100.117.204] with 32 bytes of data:

Successful Result

Reply from 100.100.117.204: bytes=32 time=4ms TTL=254

Reply from 100.100.117.204: bytes=32 time=4ms TTL=254

Reply from 100.100.117.204: bytes=32 time=3ms TTL=254

Reply from 100.100.117.204: bytes=32 time=3ms TTL=254

Ping statistics for 209.172.117.204:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 3ms, Maximum = 4ms, Average = 3ms

Failure

C:\WINDOWS\tracing>ping joule.dev.airwave.com

Pinging joule.dev.airwave.com [10.51.2.5] with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 10.51.2.5:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Appendix B: Reference HTML Post

Here is an example HTML Post that tests AMC to AMP connectivity and validates data returned from AMP to AMC. *Note modify the highlighted line to match the Hostname that is being tested.*

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
  <link rel="stylesheet" href="style.css" type="text/css" />
  <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
  <meta name="author" content="John Smith" />
  <meta name="description" content="sample of wireless client data submission" />
  <meta name="keywords" content="" />
  <title>Wireless Client Data Submission</title>
</head>
<body>

<form action="https://cp.airwave.com/wireless_client" method="post">

<input type="text" name="client_mac" value="00:00:01:00:00:01" />
<input type="text" name="client_version" value="xx.xx" />
<input type="text" name="client_ip" value="Wireless IP of Client" />
<input type="text" name="client_user" value="User Name" />
<input type="text" name="client_domain" value="Domain Name" />
<input type="text" name="client_mfg_mod" value="Card Manufacturer and Model" />
<input type="text" name="client_fw" value="Client Firmware" />

<hr />

<input type="text" name="bssid_1" value="00:00:00:00:00:01" />
<input type="text" name="ssid_1" value="foo" />
<input type="text" name="channel_1" value="1" />
<input type="text" name="rssi_1" value="foo1" />
<input type="text" name="wep_1" value="0" />

<br />

<input type="text" name="bssid_2" value="00:00:00:00:00:02" />
<input type="text" name="ssid_2" value="bar" />
<input type="text" name="channel_2" value="5" />
<input type="text" name="rssi_2" value="bar1" />
<input type="text" name="wep_2" value="0" />

<br />

<input type="text" name="bssid_3" value="00:30:65:2E:75:DB" />
<input type="text" name="ssid_3" value="dev" />
<input type="text" name="channel_3" value="11" />
<input type="text" name="rssi_3" value="0" />
<input type="text" name="wep_3" value="1" />

<br />
```

```
<input type="text" name="bssid_4" value="00:20:A6:4F:24:80" />
<input type="text" name="ssid_4" value="" />
<input type="text" name="channel_4" value="140" />
<input type="text" name="rssi_4" value="pieces" />
<input type="text" name="wep_4" value="0" />

<br />

<input type="submit" />

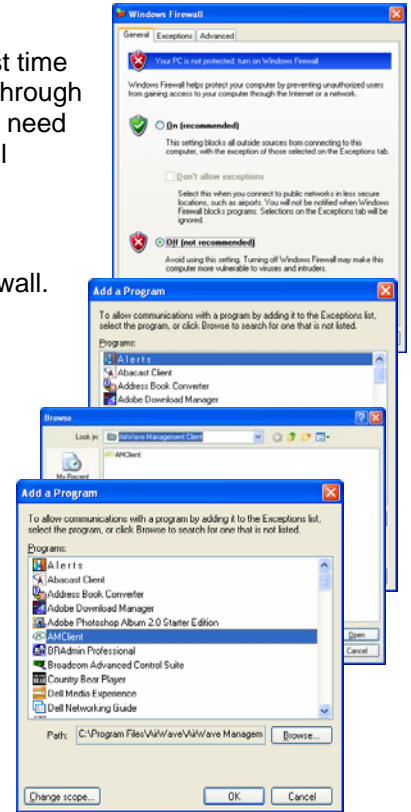
</form>

</body>
</html>
```

Appendix C: Configure MS Personal Firewall - AMC to AMP Communication

Windows XP SP2 installs a personal firewall by default. It needs to be configured to allow AMC to create outbound connections to AMP. The first time you run AMC Windows will display a popup asking if it should be allowed through the firewall. If you told the firewall to block connections from AMC you will need to reconfigure it to allow the AMC to connect to AMP. The steps below will configure Microsoft's personal firewall to allow AMC to create outbound connections from your PC.

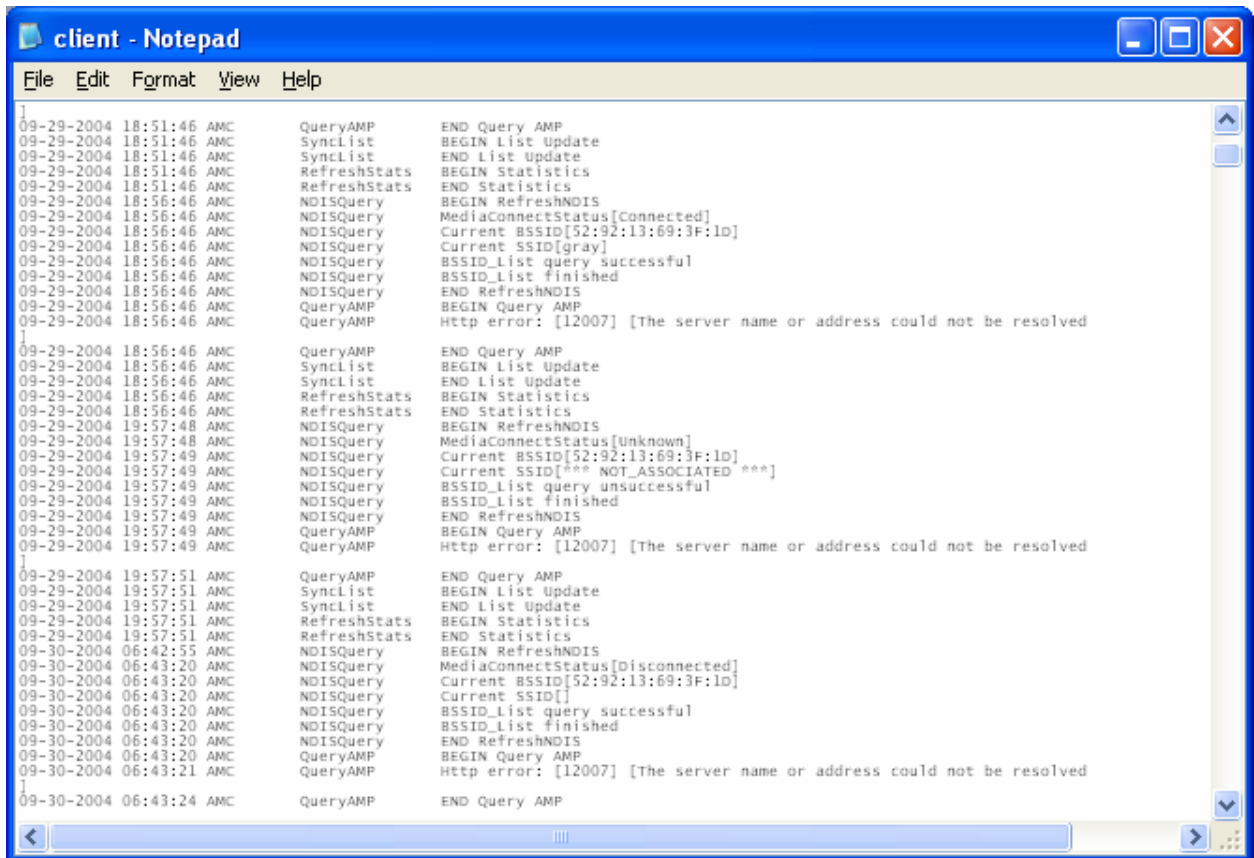
1. Navigate to Start -> Control Panel -> Security Center -> Windows Firewall.
2. Select the "Exception" Tab.
3. Select the "Add Program" Button.
4. Browse to c:\program files\Airwave\Airwave Management Client\.
5. The AMC ICON should automatically appear, because the program is searching for all executable files.
6. Double click on the AMC ICON and the AMC client will automatically be inserted in alphabetical order.
7. Click the "OK" button to save.



Appendix D: View AMC Log File

The AMC log file provides an additional mechanism to diagnose certain error conditions

1. Launch Notepad by navigating to Start→Run and type “notepad” in the prompt box.
2. Navigate to File→Open c:\Documents and Settings\All Users\Application Data\Airwave\AMClient.log.
3. Proceed to the bottom of the file.
4. Look for error messages. See the example below.



```

}
09-29-2004 18:51:46 AMC      QueryAMP      END Query AMP
09-29-2004 18:51:46 AMC      SyncList     BEGIN List Update
09-29-2004 18:51:46 AMC      SyncList     END List Update
09-29-2004 18:51:46 AMC      RefreshStats BEGIN Statistics
09-29-2004 18:51:46 AMC      RefreshStats END Statistics
09-29-2004 18:56:46 AMC      NDISQuery   BEGIN RefreshNDIS
09-29-2004 18:56:46 AMC      NDISQuery   MediaConnectStatus[Connected]
09-29-2004 18:56:46 AMC      NDISQuery   Current BSSID[52:92:13:69:3F:1D]
09-29-2004 18:56:46 AMC      NDISQuery   Current SSID[gray]
09-29-2004 18:56:46 AMC      NDISQuery   BSSID_List query successful
09-29-2004 18:56:46 AMC      NDISQuery   BSSID_List finished
09-29-2004 18:56:46 AMC      NDISQuery   END RefreshNDIS
09-29-2004 18:56:46 AMC      QueryAMP    BEGIN Query AMP
09-29-2004 18:56:46 AMC      QueryAMP    Http error: [12007] [The server name or address could not be resolved]
}
09-29-2004 18:56:46 AMC      QueryAMP    END Query AMP
09-29-2004 18:56:46 AMC      SyncList     BEGIN List Update
09-29-2004 18:56:46 AMC      SyncList     END List Update
09-29-2004 18:56:46 AMC      RefreshStats BEGIN Statistics
09-29-2004 18:56:46 AMC      RefreshStats END Statistics
09-29-2004 19:57:48 AMC      NDISQuery   BEGIN RefreshNDIS
09-29-2004 19:57:48 AMC      NDISQuery   MediaConnectStatus[Unknown]
09-29-2004 19:57:49 AMC      NDISQuery   Current BSSID[52:92:13:69:3F:1D]
09-29-2004 19:57:49 AMC      NDISQuery   Current SSID[*** NOT_ASSOCIATED ***]
09-29-2004 19:57:49 AMC      NDISQuery   BSSID_List query unsuccessful
09-29-2004 19:57:49 AMC      NDISQuery   BSSID_List finished
09-29-2004 19:57:49 AMC      NDISQuery   END RefreshNDIS
09-29-2004 19:57:49 AMC      QueryAMP    BEGIN Query AMP
09-29-2004 19:57:49 AMC      QueryAMP    Http error: [12007] [The server name or address could not be resolved]
}
09-29-2004 19:57:51 AMC      QueryAMP    END Query AMP
09-29-2004 19:57:51 AMC      SyncList     BEGIN List Update
09-29-2004 19:57:51 AMC      SyncList     END List Update
09-29-2004 19:57:51 AMC      RefreshStats BEGIN Statistics
09-29-2004 19:57:51 AMC      RefreshStats END Statistics
09-30-2004 06:42:55 AMC      NDISQuery   BEGIN RefreshNDIS
09-30-2004 06:43:20 AMC      NDISQuery   MediaConnectStatus[Disconnected]
09-30-2004 06:43:20 AMC      NDISQuery   Current BSSID[52:92:13:69:3F:1D]
09-30-2004 06:43:20 AMC      NDISQuery   Current SSID[]
09-30-2004 06:43:20 AMC      NDISQuery   BSSID_List query successful
09-30-2004 06:43:20 AMC      NDISQuery   BSSID_List finished
09-30-2004 06:43:20 AMC      NDISQuery   END RefreshNDIS
09-30-2004 06:43:20 AMC      QueryAMP    BEGIN Query AMP
09-30-2004 06:43:21 AMC      QueryAMP    Http error: [12007] [The server name or address could not be resolved]
}
09-30-2004 06:43:24 AMC      QueryAMP    END Query AMP

```

5. Be aware that once a log reaches 4 MB in size, the old log information is backed up to the AMClient.bak file in the same directory. You may need to search this file to gather all relevant information, depending on the time and date the error occurred .
6. If you are still having problems, email support@airwave.com with “AMC Problem” in the Subject Line and include the AMClient.log as a file insert.