

# **AirWave Management Client 8.0**



User Guide

## Copyright

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

## Warranty

This hardware product is protected by an Aruba warranty. For details, see the Aruba Networks standard warranty terms and conditions.

<b>Chapter 1 Overview</b>	<b>5</b>
AWMS Requirements	6
Client Requirements	6
<b>Chapter 2 Configuring AMP for AMC Management Client</b>	<b>7</b>
Add/Validate Role	7
Add/Validate Client User	8
<b>Chapter 3 Installing AirWave Management Client</b>	<b>11</b>
Download AMC	11
Installation Procedure	11
<b>Chapter 4 Leveraging AMC as an Additional Scanner</b>	<b>12</b>
How AMC Works	12
How AMP Processes AMC Information	12
<b>Chapter 5 Utilizing AMC Standalone</b>	<b>14</b>
Locating Rogue or Managed Devices	14
Process	14
Client Connectivity Security	16
PCI Compliance	16
QoS Wireless Mean Opinion Score (MOS)	17
MOS Calculation Percentages	18
AP Provisioning	18
Location Testing	19
Authentication and DHCP Time Calculations	19
Speed Test	20
<b>Chapter 6 Configuring Windows Firewall</b>	<b>21</b>
<b>Chapter 7 Sample Input Data from AMC</b>	<b>24</b>



The AirWave Management Client™ (AMC) is a Windows software utility that enables a client device, like a laptop, to act as a passive RF sensor and augment the AirWave Wireless Management Suite's (AWMS) Rogue Access Point Intrusion Detection System (RAPIDS) module. The AirWave Management Client can improve both wireless network security and performance.

**Table 1:** *AirWave Management Client Features*

Feature	Description
Increase PCI Compliance	After every AMC-enabled client device becomes an additional RF sensor, it increases the scanned coverage area, decreases the time of initial discovery, and increases location capability.  AMC also logs every association while providing a detailed and summary report based on the amount of time the client has been connected to PCI-compliant networks.
Avoid Man-in-the-Middle Attack	The AMC displays a list of all APs/BSSIDs 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 secured, managed devices.
Minimize RF Interference	The 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.
Increase Rogue Location	The AMC provides a <b>Hunt</b> button, which scans more frequently, and provides a beep based on signal quality. This enables faster location of a rogue device. See <a href="#">"Locating Rogue or Managed Devices"</a> on page 14 for details.
Enhance Planning	The AMC hunting feature can also help locate managed devices that are already mounted on the ceiling but have not been provisioned onto a floor plan within VisualRF.
Increase QoS Visibility	The AMC provides a wireless Mean Opinion Score (MOS) score based on latency, signal quality, and data rate. This information is stored and can be exported to .CSV for reporting.
Client authentication/DHCP time calculation	The AMC provides a <b>Renew IP/Auth</b> button. Clicking this calculates the authentication and DHCP time when you refresh a wireless network connection. Authentication time is the time taken by the device to reauthenticate to the network and DHCP time indicates the time taken to obtain the IP address of the device after the successful authentication occurs.
Client speed	The AMC provides a <b>Speed</b> button. Clicking this detects the speed of the wireless card's connection on the client computer.
Location test	The AMC provides a <b>Locate</b> button. Clicking this gives an

**Table 1:** *AirWave Management Client Features (Continued)*

Feature	Description
	approximate determination of the physical location of the rogue access point and the device. Beeping and frequency in the AMC client is based on proximity of the rogue access point with the device.

## AWMS Requirements

- AMP Version 7.1 or later
- AirWave Management Platform (AMP) server's IP address or hostname
- A client role configured with type AirWave Management Client
- A client user associated to the client role
- HTTPS (port 443) connectivity between the client device and the AMP server

## Client Requirements

- Supported Operating Systems:
  - Windows® XP
  - Windows Vista®
  - Windows 7
  - Windows 8
- Wireless NIC
- 1 GB of RAM
- 20 MB of disk space

AMC utilizes NDIS within the Microsoft® framework, so any card that works with Microsoft supports AMC.

A client user must be configured with a proper role assigned to properly and securely connect to an AMP server, .

### Add/Validate Role

1. Navigate to the **AMP Setup > Roles** page.
2. Ensure there is a role with type AirWave Management Client defined.  
Perform the following steps if a role does not exist:
  - a. Click the **Add** button.
  - b. Enter **AMC Client** as the name.
  - c. Select **AirWave Management Client** as the type.
  - d. Specify whether to allow users of this role to disable timeout. This defaults to No.
  - e. Click **Add** to create the role, as in [Figure 1](#) below.

**Figure 1: Add/Validate Role**

**Add** New Role

	Name ▲	Enabled	Type	Access Level
	Admin	Yes	AMP Administrator	-
	AMC Client	Yes	AirWave Management Client	-
	Help-Desk	Yes	AP/Device Manager	Monitor (Read Only)
	helpdeskonly	Yes	AP/Device Manager	Monitor (Read Only)
	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)

5 Roles  
Select All - Unselect All

**Delete**

**Role**

Name:

Enabled: ☒ Yes ☐ No

Type:

AP/Device Access Level:

Top Folder:

RAPIDS:

VisualRF:

Aruba Controller Role:

Display client diagnostics screens by default: ☐ Yes ☒ No

Allow user to disable timeout: ☐ Yes ☒ No

Allow reboot of APs/Devices: ☐ Yes ☒ No

**Guest User Preferences**

Allow creation of Guest Users: ☒ Yes ☐ No

Allow accounts with no expiration: ☒ Yes ☐ No

Allow sponsor to change sponsorship username: ☐ Yes ☒ No

Custom Message:


**Add** **Cancel**

## Add/Validate Client User

1. Navigate to the **AMP Setup > Users** page.
2. Check that there is a client user assigned to the AMC client role.  
Perform the following steps if the client user does not exist (see [Figure 2](#) below):
  - a. Click **Add**.
  - b. Enter **client** in the Username field.
  - c. Select **AirWave Management Client** as the role.
  - d. Enter the password.
  - e. Click **Add**.

If necessary, perform the following steps to change the client user's password.



- Click the pencil icon  next to the client row.
- Enter the new password.
- Click the **Save** button to save your changes.



The AMC password must correspond with the client password in order to establish communication between AMP and the AirWave Management Client. The user name must match the client. AMC is included on every AMP server.

**Figure 2: Add/Validate Client User**

Add
New User

	Username ▲	Role	Role Enabled	Type
<input type="checkbox"/>	admin	Admin	Yes	AMP Administrator
<input type="checkbox"/>	Client	AMC Client	Yes	AirWave Management Client
<input type="checkbox"/>	Help	Read-Only Monitoring & Auditing	Yes	AP/Device Manager
<input type="checkbox"/>	helpdesk	Help-Desk	Yes	AP/Device Manager
<input type="checkbox"/>	helpdeskonly	helpdeskonly	Yes	AP/Device Manager

5 Users

Select All - Unselect All

Delete

**User**

Username:

Role: 

Help-Desk ▼

Enabled: ☒ Yes ☐ No

Password:

Confirm Password:

Name:

Email Address:

Phone:

Notes:

Add
Cancel



## Download AMC

AMC is included on every AMP server.

1. Navigate to the **Home > Documentation** page.
2. Under the **RAPIDS** section, select the **Download AirWave Management Client** link.
3. Click **Run** when presented with the Windows File Download dialog.

## Installation Procedure

The AMP password entered here must match the AMP password that you configured in ["Add/Validate Client User"](#) on [page 8](#).

1. The AMC Setup Wizard dialog box displays when the installation begins. Click **Next**. The **License Agreement** dialog box displays.
2. Review the license agreement thoroughly. Select the **I Agree** option and then click **Next** to continue. Click **Do Not Agree** to terminate the installation. The **Select Installation Folder** dialog box displays.
3. Enter the path for this installation. You can also click the **Disk Cost** button to optionally check the disk cost. Click **Next** to continue. The **AMP Login Information** dialog box displays.
4. Enter the AMP hostname or IP address and enter the password. Click **Next** to continue. The **Confirm Installation** dialog box displays.
5. Click **Next** to continue. After the AMC installation is complete, the **Installation Complete** dialog box displays.
6. Click **Close**.

On startup, AMC runs minimized in your task tray. This is indicated by the presence of the AirWave icon in the task tray.

One of the important features of the AMC is to provide PCI compliance. Some locations in the enterprise may have legacy wireless APs that do not scan or there is no wireless at all. Even if the locations have modern (scanning) APs, they may not provide full coverage for the entire facility.

AMC meets the PCI scanning requirements by augmenting modern APs scanning or as the primary scanning source. You can deploy AMC on some or all laptops in the locations that need help with PCI compliance. The AMC runs unattended, scanning the air space, and reporting back to AMP on a continuous basis.

## How AMC Works

The process can be summarized as follows:

1. By default AMC queries NDIS for a list of BSSIDs every 5 minutes.
2. AMC posts (via HTTPS) the list of BSSIDs to AMP along with:
  - MAC address of the device
  - Device Manufacturer
  - Device Model
  - Device Operating System
  - Device Operating System details
  - Name
  - Username
  - Phone number
  - GPS and GPS timestamp
  - Serial number
  - Description of the WLAN adapter
  - Association
  - QoS
  - BSSID timestamp
3. AMP responds to the post with the following information:
  - BSSID
  - Rogue Classification

## How AMP Processes AMC Information

The RAPIDS module receives the list of BSSIDs and responds with a rogue classification for each BSSID. Next, RAPIDS processes each of the BSSIDs as discovery events.

Perform the following steps to view AMC discovery events in AMP:

1. Navigate to the **RAPIDS > List** page.
2. Filter on high-threat rogues by selecting the proper Rules Classification or Threat Level.
3. Select a rogue device, such as the 3Com example [Figure 3](#) below.

**Figure 3: RAPIDS Detail Summary**

Name:	Aruba Netw-61:3C:C0	Model:	-	First Discovered:	10/26/2010 3:48 PM
Acknowledge:	<input type="radio"/> Yes <input checked="" type="radio"/> No	IP Address:	10.1.84.31	First Discovery Method:	Wireless AP scan
Controller Classification:	Valid	Confidence:	100		
WMS Classification Override:	Unclassified				
SSID:	sw-gwang-mon5	First Discovery Agent:	-		
RAPIDS Classification:	Valid	Channel:	40	Last Discovered:	4/3/2014 2:16 PM
Classification Rule:	Aruba Lab APs running encryption	WEP:	Yes	Last Discovery Method:	Switch/Router Bridge Forwarding Table Data
RAPIDS Classification Override:	- No Override -	WPA:	No	Last Discovery Agent:	1344-core1
Threat Level:	5	Network Type:	AP	Signal:	-24
Threat Level Override:	1				
Radio MAC Address:	00:0B:86:61:3C:40	Current Associations:	0		
Radio Vendor:	Aruba Networks	Max Associations:	2		
LAN MAC Address:	00:0B:86:61:3C:C0				
LAN Vendor:	Aruba Networks				
QUT Score:	3 (Override score)				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				
Notes:					

[Refresh](#) this page for updated results.

The RAPIDS Detail summary provides:

- LAN/Radio MACs
- Vendor
- Operating System
- First/Last discovery date/time
- Characteristics, such as channel, signal, security

A table below the summary section shows all discovery events, as in [Figure 4](#) below. AMC discovery events are listed in the Discovery Method column as Wireless AirWave Management Client scan.

**Figure 4: RAPIDS Detail Discovery Events**

1-6 of 6 Discovery Events Page 1 of 1 [Reset filters](#) [Choose columns](#) [Export CSV](#)

RSSI	Signal	Channel	SSID	WEP	WPA	BSSID	Network Type	IP Address	Time	Discovery Method	Discovery Agent	Port
16	-74	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/31/2013 4:03 AM	Wireless AP scan	hello-there	-
15	-74	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/31/2013 4:03 AM	Wireless AP scan	6cf3:7fce:c5:b8	-
27	-69	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/31/2013 3:58 AM	Wireless AP scan	00:24:6c:c7:f8:1c	-
23	-89	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/31/2013 3:52 AM	Wireless AP scan	spectrum monitor	-
28	-60	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/31/2013 3:51 AM	Wireless AP scan	ARUBANETWORKS/test	-
28	-55	6	instant	No	No	24:DE:C6:88:92:C2	AP	-	5/30/2013 11:51 PM	Wireless AP scan	00:24:6c:c8:6e:e0	-

1-6 of 6 Discovery Events Page 1 of 1 [Reset filters](#)

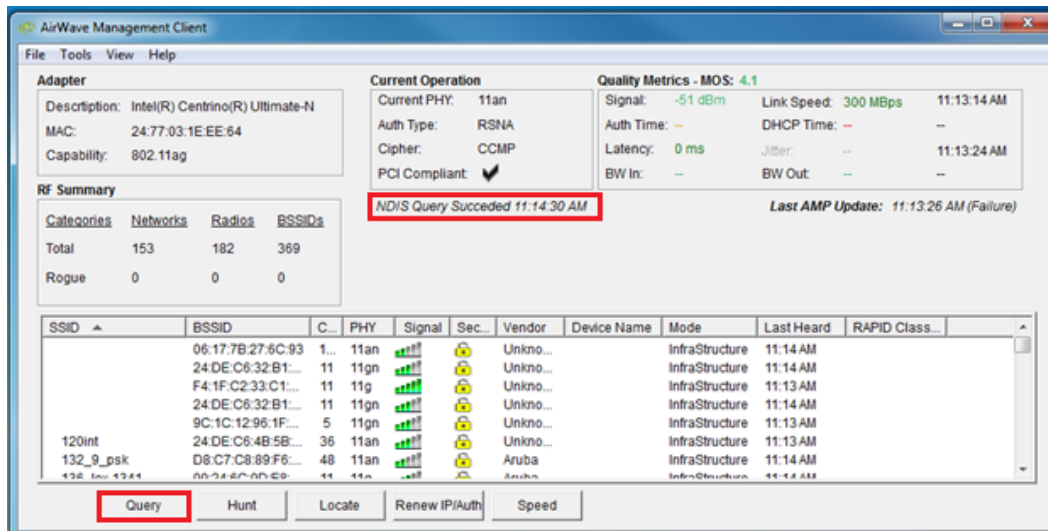
The AMC scans for events including the following information:

- **Discovery Agent** - the device name of the scanning client
- **Time** - The last date/time the AMC client posted to AMP
- **Rogue Characteristics** - signal, channel, security, port, and so on

AMC includes the following security advantages:

- "Locating Rogue or Managed Devices" on page 14
- "Client Connectivity Security" on page 16
- "QoS Wireless Mean Opinion Score (MOS)" on page 17
- "AP Provisioning" on page 18
- "Location Testing" on page 19
- "Authentication and DHCP Time Calculations" on page 19
- "Speed Test" on page 20

**Figure 5: Query**



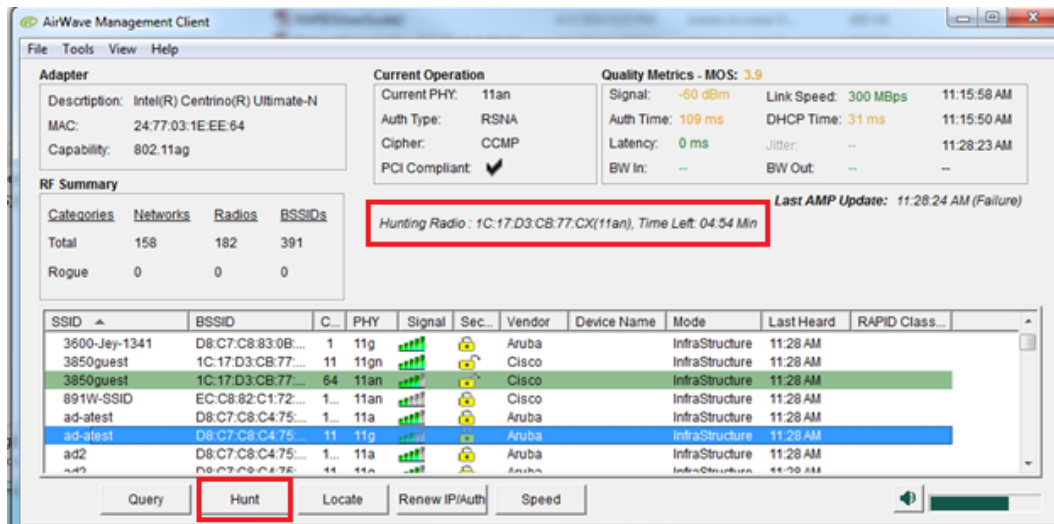
## Locating Rogue or Managed Devices

AMC supports a device hunting feature that provides SONAR-like functionality by audibly indicating proximity to the selected device.

### Process

- Find a BSSID that you want to hunt.
- Sort based on BSSID.
- Click **Hunt**.

**Figure 6: Hunt**



You will notice the following events:

- Beeping and frequency based on proximity to rogue device.
- If you have correctly configured the VisualRF on an AMP, you can see the client and rogue AP locations.
- A new widget in the bottom right of the window visually indicating proximity to the rogue device.
- AMC highlights the hunted BSSID in blue.
- AMC automatically highlights in green and searches for all BSSIDs broadcasting on the radio for the selected BSSID.

In the background, AMC facilitates the following:

- Querying NDIS every six seconds.
- Setting the Hunt Timer to five minutes.
- Flushing the cache after every NDIS query.
- Disabling posting of BSSIDS to AMP as not to overwhelm the server.
- Begin beeping based on signal as shown in [Table 2](#) below.

**Table 2: Signal Quality and Beep Frequency**

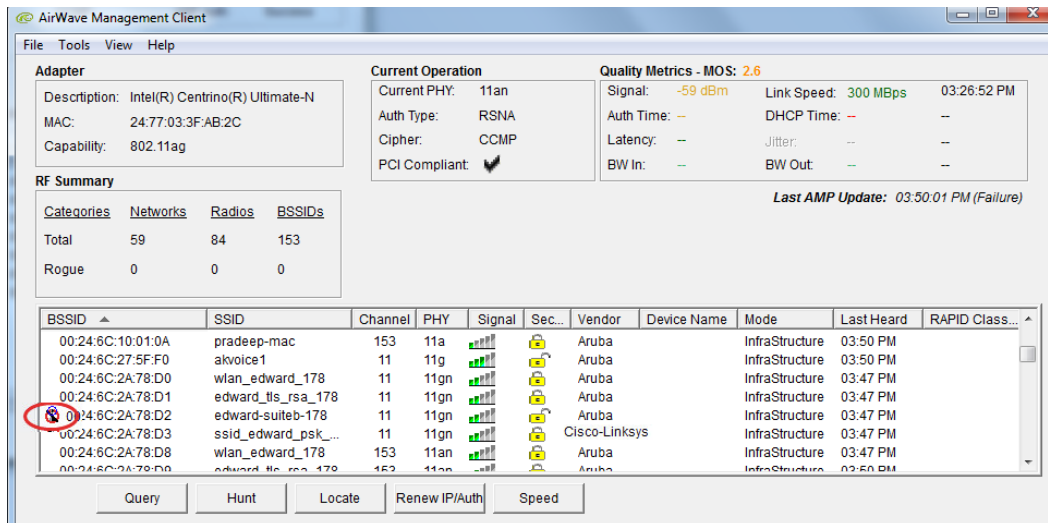
Signal Quality	Frequency
Better than -46	5 beeps per second
-46 to -55	2.5 beeps per second
-56 to -65	1 beep per second
-66 to -75	1 beep every 2 seconds
-76 to -85	1 beep every 3 seconds
-85 to -95	1 beep every 4 seconds
Less than -95	1 beep every 5 seconds

## Client Connectivity Security

AMC can be used as a standalone security tool to ensure your WLAN connectivity is protected. You can quickly eliminate man-in-the-middle attacks. In the example below, the client device is associated with **corp-ssid**, but the vendor is a third party and the corporate standard WLAN infrastructure provider is Aruba Networks. An unauthorized user has maliciously configured a small office and home office (SOHO) access point with the same SSID to decoy unsuspecting employees onto this rogue network.

The above example is very common at coffee shop WLAN installations.

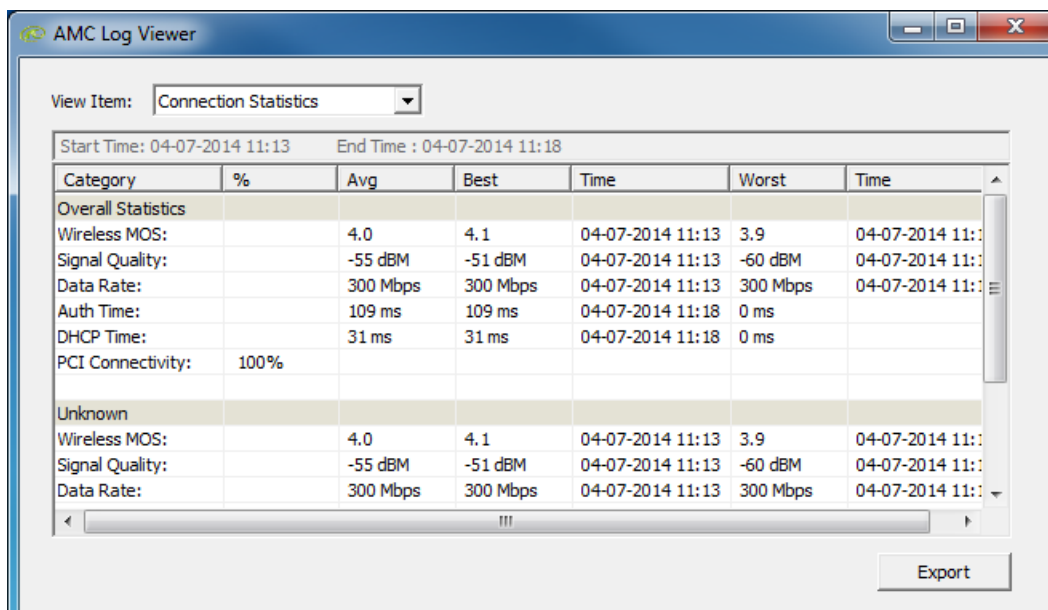
**Figure 7: AMC Man-in-the-Middle Example**



## PCI Compliance

AMC tracks the percentage of time when your laptop is connected to a PCI compliant SSID. To view your PCI compliance history, navigate to **View Logs** and select **Connection Statistics** within the **View Item** drop-down list, as in [Figure 8](#) below. The last row under the **Category** column contains the percentage of time that your laptop was associated with a PCI-compliant SSID.

**Figure 8: AMC Log Viewer**





## QoS Wireless Mean Opinion Score (MOS)

AMC calculates a wireless MOS score based on the information in .

**Table 3:** *Latency, Data, Signal, Auth, and DHCP*

Category	11g	11a	11ng	11na	Notes
<b>Latency Values (ms)</b>					
5	10	10	10	10	10 or less
4	25	25	25	25	Between 11 and 25
3	50	50	50	50	Between 26 and 50
2	100	100	100	100	Between 51 and 100
1					less than 100
<b>Data Values (mbps)</b>					
5	48	54	150	250	48 or above
4	36	48	100	150	Between 5 and 4
3	24	36	75	100	Between 4 and 3
2	18	24	50	75	Between 3 and 2
1					Less than 2
<b>Signal Values (dBm)</b>					
5	-45	-45	-45	-45	-45 or less
4	-55	-55	-55	-55	Between -46 and -55
3	-70	-70	-70	-70	Between -55 and -70
2	-85	-85	-85	-85	Between -71 and -85
1					Less than -85
<b>Auth Values (ms)</b>					
5	25	25	25	25	25 or above
4	50	50	50	50	Between 26 and 50
3	100	100	100	100	Between 56 and 100
2	500	500	500	500	Between 101 and 500
1					Less than 500

**Table 3: Latency, Data, Signal, Auth, and DHCP (Continued)**

Category	11g	11a	11ng	11na	Notes
DHCP Values (ms)					
5	10	10	10	10	10 or above
4	20	20	20	20	Between 11 and 20
3	40	40	40	40	Between 21 and 40
2	75	75	75	75	Between 41 and 75
1					Less than 75

## MOS Calculation Percentages

- Data rate counts 20%.
- Latency counts 40% or 2 of 5.
- Signal counts 20% or 1 of 5.
- Auth counts 10%.
- DHCP counts 10%.

You can view historical MOS score by navigating to **View > Logs**.

## AP Provisioning

You can use AMC to provision the access points (AP) in a wireless network. This allows you to provision AP even before connecting to a controller.

1. Click **Tools** and select **Provision Aruba Thin AP**. Refer to [Figure 9](#) below.

**Figure 9: AP Provisioning**

Provision AP

Communication

Com Port:  ☐ Do not connect to COM port

General

☐ Always enter AP boot mode

☒ Remote AP ☐ Campus AP

☐ With Certificate

Authentication

Remote AP

Pap user:  Pap password:  Confirm Pap pwd:

IKE password:  Confirm IKE pwd:

802.1X user:  Password:  Confirm pwd:

PPPoE

User:  Service Name:

Password:  CHAP secret:

Confirm pwd:  Confirm CHAP secret:

Network

☒ Obtain IP Address using DHCP

Antenna

☐ AP has external antenna

2.4 GHz Ant. Gain:  5 GHz Ant. Gain:

Connected to serial port

Command Line Instructions

Click Apply Button OR Copy text and paste into terminal emulator software like putty etc

Serial out from Port

2. Connect the AP to a serial console.
3. Provide inputs for mandatory provision items and then click **Generate**.

A list of commands are generated which are shown in the right top area. You can generate the commands even without connecting the AP to the console.

If you want AMC to push the command:

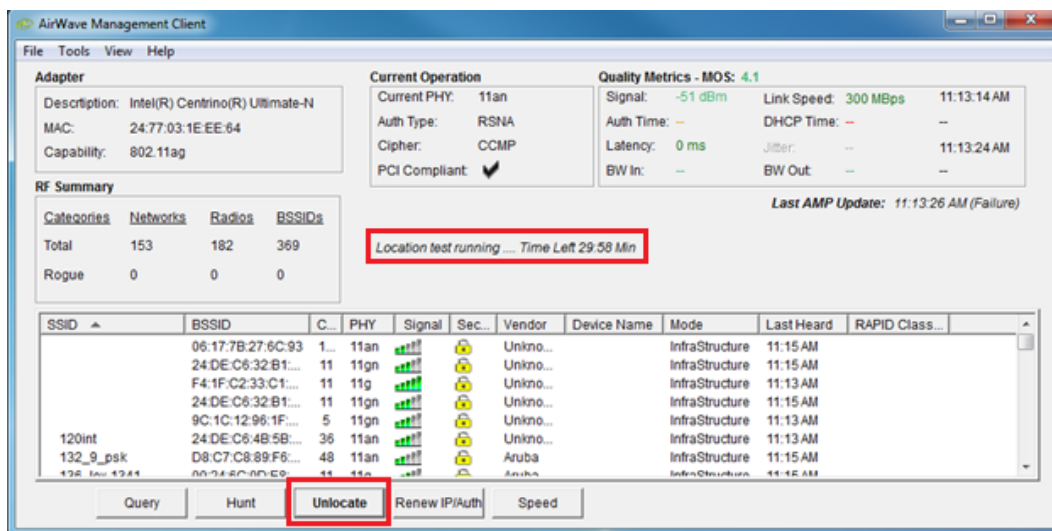
1. Connect the AP to serial console.
2. Close all the terminal applications to the particular com port AP provision window on AMC.
3. Enter the required fields and click **Generate**.
4. Click **Apply**.

You can view the serial output data on the lower-right side of the window.

## Location Testing

This feature allows the VisualRF component of the AMP to correctly identify the client location. When you click **Locate**, the client sends the BSSID information to AMP frequently. Clients send the RSSI information to calculate the VisualRF location correctly. See [Figure 10](#) below.

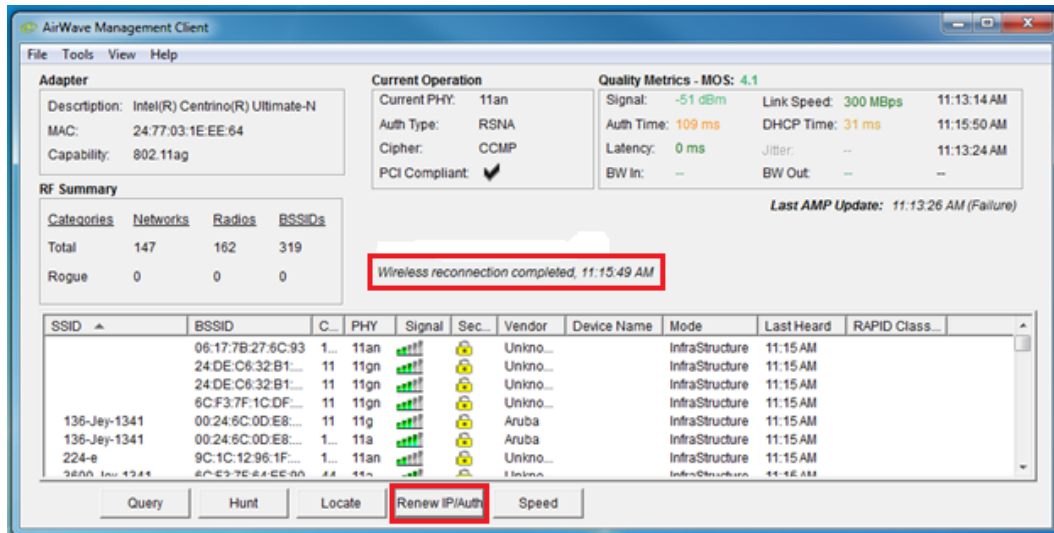
**Figure 10: Location Testing**



## Authentication and DHCP Time Calculations

AMC can be used to calculate the authentication and DHCP time when you refresh a wireless network connection. Authentication time is the time taken by the device to reauthenticate to the network and DHCP time indicates the time taken to obtain the IP address of the device after the successful authentication occurs. To reauthenticate, click **Renew IP/Auth**.

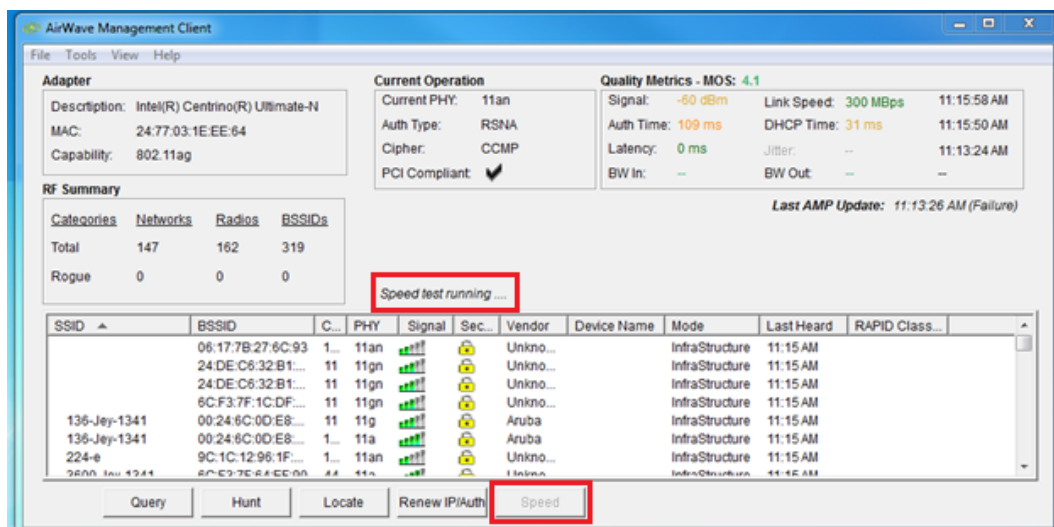
Figure 11: Renew IP/Auth



## Speed Test

This feature identifies the quality of network connection by calculating bandwidth in (BW in) and bandwidth out (BW out) fields with respect to latency server configuration. The AMP acts as a bandwidth server. To determine the speed, click **Speed**. See Figure 12 below.

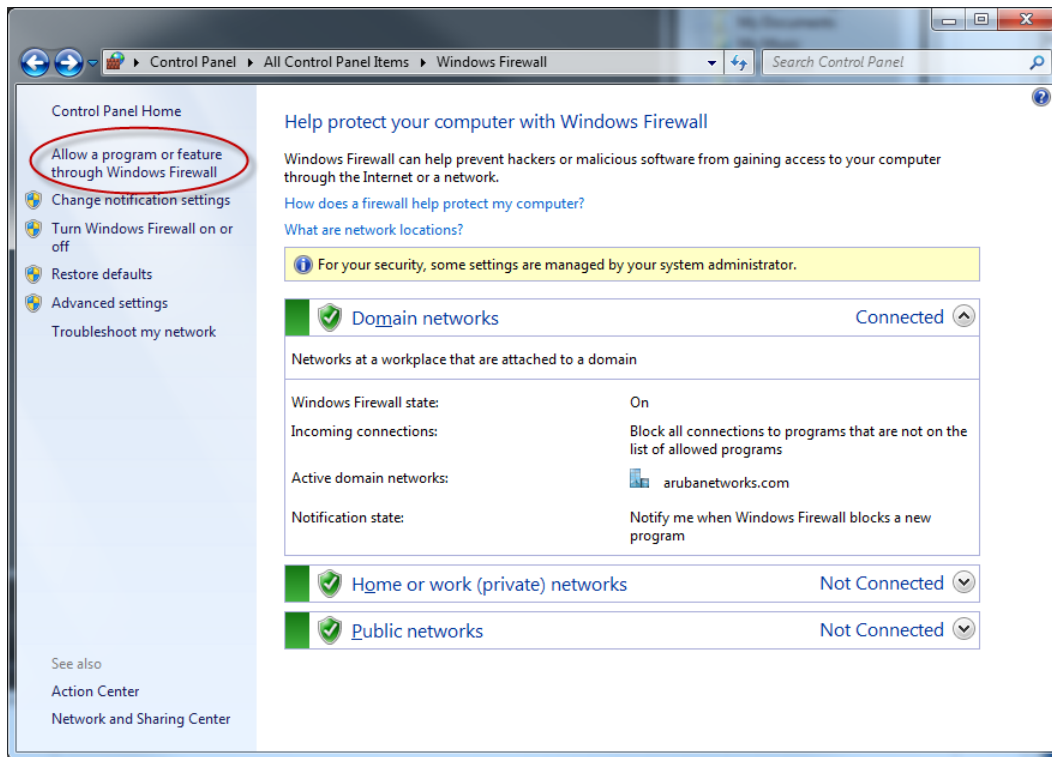
Figure 12: Speed Test



The following example shows how to allow the AMC program to run through Windows Firewall in Windows 7. Refer to your operating system's documentation for information about how to do this for other versions.

1. Go to **Control Panel > All Control Panel Items > Windows Firewall**.
2. In the left navigation, click the **Allow a program or feature through Windows Firewall** link, as in [Figure 13](#) below.

**Figure 13:** *Windows Firewall Settings*



3. A list of allowed programs displays as shown in [Figure 14](#) below.



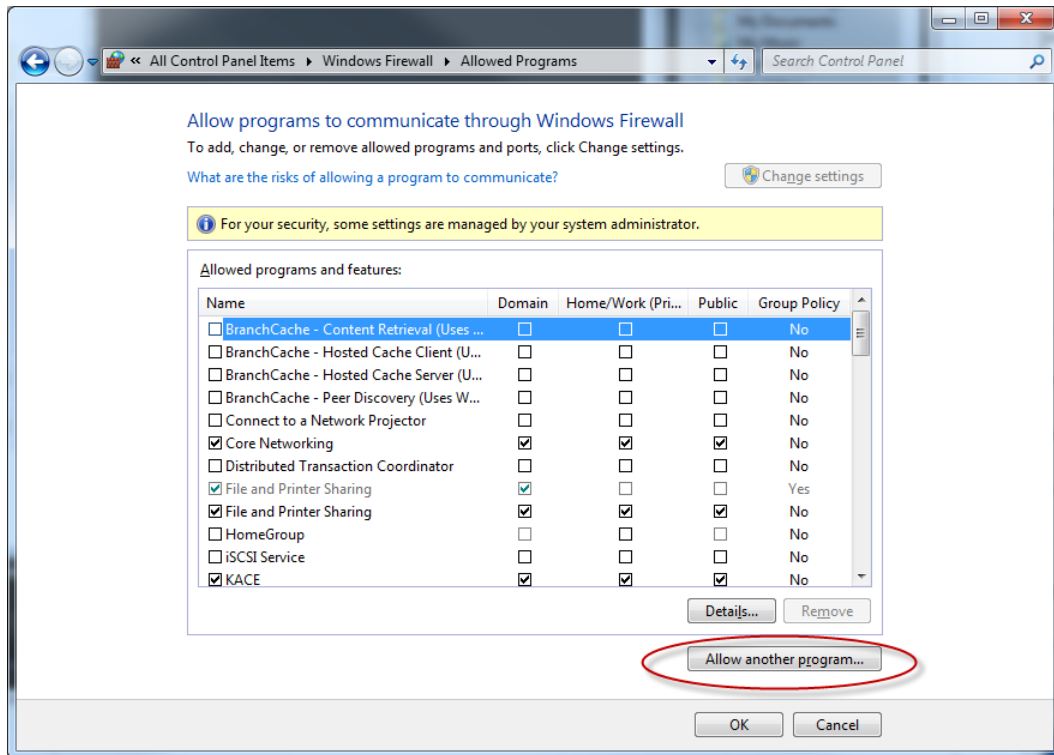
---

If **AMC** is not available in the list of allowed programs, then click **Allow another program**.

---

4. Note that if **AMC** is not available in the list of allowed programs, then click the **Allow another program** button.

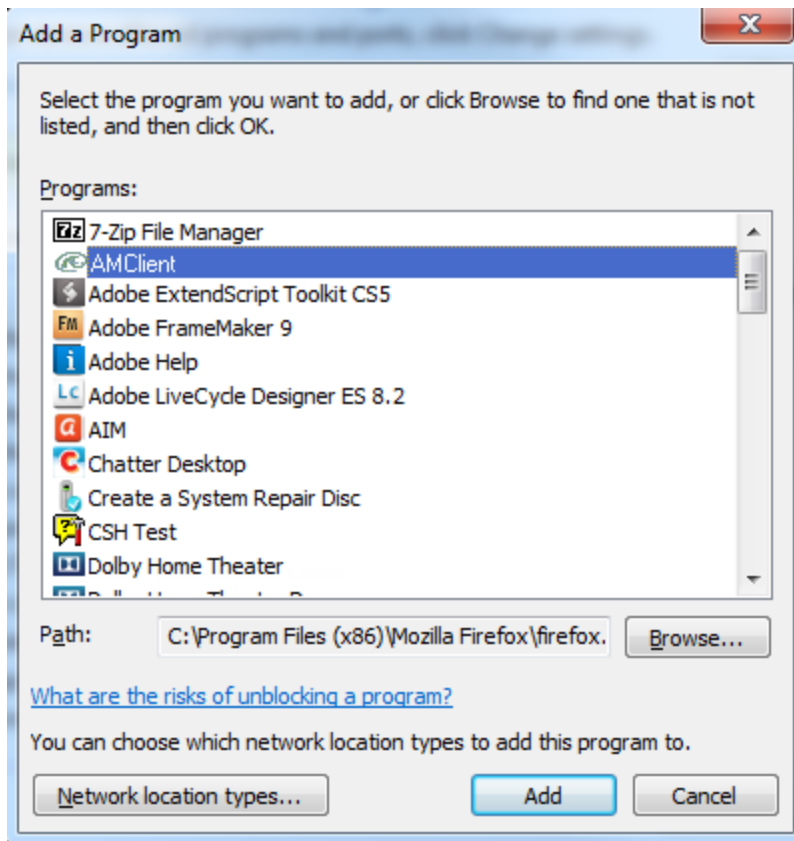
**Figure 14:** *Allowed programs*



The **Add a Program** dialog box displays.

5. Select **AMC** if it is available, or click the **Browse** button to locate it on your system.

**Figure 15:** *Add a Program dialog box*



6. Click **Add** when you are finished.

Upon successful completion, AMC is available in the list of allowed programs and features. Be sure that the appropriate check boxes are selected (Domain, Home/Work, or Public).

This section includes a sample input of data from the AMC file that tests AMC to AMP connectivity and validates data returned from AMP to AMC.

```
{
  "serial_number" : "nepotists-pynot",
  "qos" : [
    {
      "timestamp" : 1302201725.4665,
      "latency" : 7.2139556
    },
    {
      "auth_time" : 46.14853755,
      "timestamp" : 1302201750.303
    },
    {
      "timestamp" : 1302201776.5145,
      "dhcp_time" : 86.97059349
    },
    {
      "bw_in" : 1.6817743,
      "timestamp" : 1302201796.4184,
      "bw_out" : 1.72081313
    }
  ],
  "device_model" : "blackfins-Chiasmodontidae",
  "association" : {
    "ip" : "10.63.181.134",
    "radio_mode" : "g",
    "channel" : 6,
    "link_speed" : 19,
    "signal" : -48.7415,
    "timestamp" : 1302201614.52523,
    "bssid" : "88:88:B2:0E:52:AF",
    "cipher" : null,
    "security_mode" : 1,
    "ssid" : "diiodide-pigmentary"
  },
  "gps_timestamp" : 1302296325.16096,
  "mac" : "88:88:47:F1:5E:A2",
  "bssids" : [
    {
      "signal" : -57.7465,
      "bssid" : "88:88:06:C3:73:06",
      "classification" : 1,
      "channel" : 11
    },
    {
      "signal" : -19.791296,
      "bssid" : "88:88:79:28:A5:A1",
      "radio_mode" : "N",
      "security" : 4,
      "classification" : 1,
      "channel" : 149,
      "network_type" : 3,
      "ssid" : "camouflagers-travelled"
    }
  ],
}
```



```
{
  "signal" : -22,
  "bssid" : "88:88:EC:2C:CB:68",
  "radio_mode" : "b",
  "security" : 2,
  "classification" : 1,
  "channel" : 3,
  "network_type" : 4,
  "ssid" : "ustilago-above-water"
}
],
"device_os" : "Windows 7",
"name" : "subentire-stick-at-it-ive",
"phone_number" : "9178999759",
"bssids_timestamp" : 1302201316.847,
"amc_version" : "all-triumphing-sketchable",
"username" : "sporocyst\\resatisfy",
"device_manufacturer" : "pancreases-Barnhard",
"gps" : "82.6853,-88.1478,722.5055",
"device_os_detail" : "6.1.7601",
"wlan_adapter_desc" : "bernoo-lenticonus"
}
```