AirWave 8.2.x and RAPIDS

User Guide

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code.

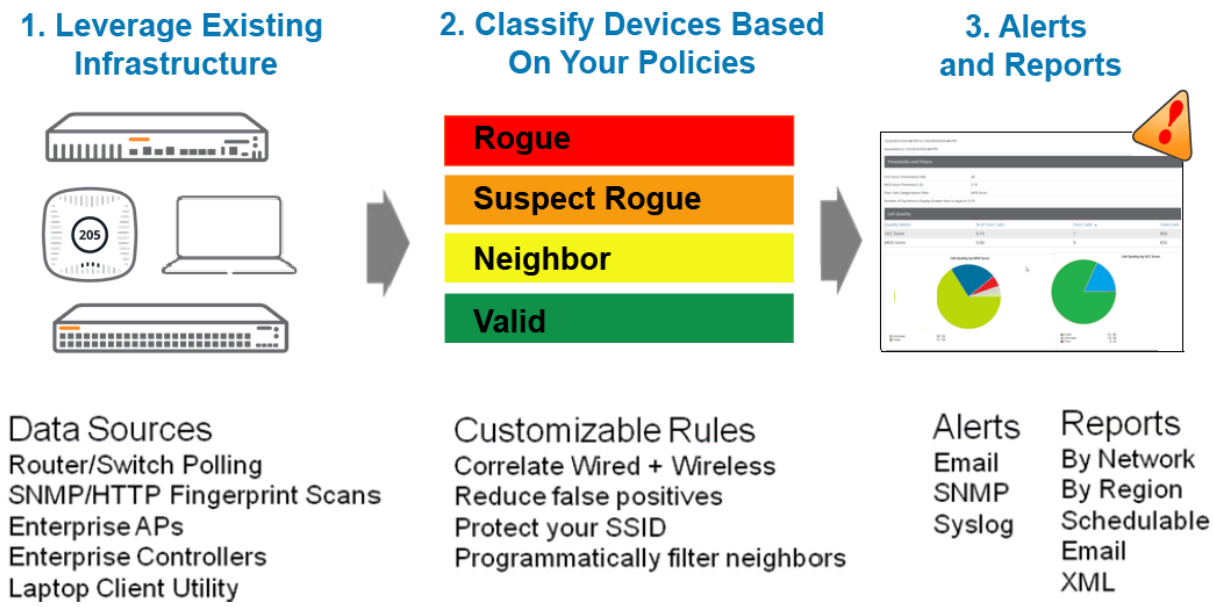
You may also request a copy of this source code free of charge at: http://hpe.com/software/opensource.

Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

This document provides best practices for leveraging the Rogue Access Point Detection (RAPIDS) module of the AirWave Wireless Management Suite (AWMS) to secure your network. RAPIDS is designed to identify and locate wireless threats by leveraging all of the information available from the infrastructure (see Figure 1). RAPIDS takes the information it collects and feeds it through a customizable set of classification rules, isolating the threat devices based on your security concerns. RAPIDS can be configured to alert administrators via email, SNMP traps, or syslog messages after a threat is identified.

Figure 1: *RAPIDS Overview*



The first step to securing your network is determining what constitutes a security threat worth investigating. Every company and organization has a different set of security needs. There are a number of factors to consider when determining a security risk. Some of the most common factors are:

- Compliance requirements (PCI, HIPAA, SOX, etc.)
- Deployed environments
- Cost of removing threats

The next step is to determine what the appropriate response to detected threats are.

- How quickly should the rogue device be removed from the network?
- Should the user who placed the rogue be educated about the dangers of rogue devices?
- Should the device be confiscated?
- How does your organization feel about wireless containment?
- How long should rogue discovery information be stored?

Many organizations believe wireless containment constitutes a breach of FCC regulations and is illegal, while others feel that it is within their rights to contain any wireless network within their facility. Please consult with your legal department to determine your enterprise's guidelines.

Common Security Threat Red Flags

Wired and Wireless

Any unmanaged device plugged into the wired network and broadcasting a signal is worth investigating. Investigating such a device is a good solution for dense environments like cities or large office buildings.

Wireless Above > -75 Signal

Any device broadcasting with a signal quality that is sufficiently strong will be investigated. A strong signal often indicates that a device is inside your organization's walls. Investigating devices that are broadcasting at a signal strength of >-80 signal can be beneficial for campuses that are fairly remote and will not see a lot of legitimate neighbor devices.

Wireless With a Managed SSID

Enterprise's SSIDs are typically managed by your IT department. No unauthorized access points should be using SSIDs. AirWave strongly recommends that any device using enterprise SSIDs should be classified as a rogue and investigated immediately. Attackers will often deploy "Honey Pot APs" using managed SSIDs in an attempt to lure valid clients to associate with them and attempt to login. It is very easy for well meaning users to accidentally attempt to login to the foreign system using their corporate credentials. Once the attacker has those credentials, they can easily access the wireless network.

Wireless With More Than Three Detecting APs

The number of detecting APs is another method for determining if a rogue is inside your premises. If only a few APs detect the device, it is very likely outside of the network and is a neighboring AP. If it is heard by a large number of APs, there is a much higher chance that the device is inside the building. Determining the number of detecting is a good method to use for campuses with single tenants. Shared office buildings might have neighbor APs on the floors above or below them that will be detected by a number of core APs.

RAPIDS has a number of configurable options. The sections below outline a number of the recommended settings that will help you get the most out of RAPIDS. The recommended settings are general and might not apply to all customers.

Wired-to-Wireless MAC Address Correlation (0-8 bits)

The Rogue MAC Address Correlation setting is used to correlate wireless discovery events with wired MAC addresses. The recommended setting is eight bits. If the two addresses are within the bit mask, they will be combined into one device record in RAPIDS. A setting of eight bits will match addresses that have the same first eight characters (00:11:22:33:44:XX). Four bits will match addresses that have the same first nine characters. Newer SOHO device LAN MAC addresses tend to be fairly far from the radio addresses. A setting of eight will combine more devices. The higher you set this value, the more likely you will see an incorrect correlation.

Wireless-to-Wireless BSSID Correlation (0-8 bits)

The wireless BSSID correlation setting is used to correlate BSSIDs from a single physical radio into one record. The recommended setting is four bits. Generally, BSSIDs increment by one on a radio and will be very close together. Because of this, we recommend four instead of eight as the setting for wireless-to-wireless correlation.

Delete Rogues not Detected for: 0-14 Days

If a rogue device has not been detected for the specified number of days, it is likely that the device is gone. The recommended setting is 14 days. Removing it from RAPIDS automatically will decrease the number of devices requiring investigation and tracking. If a device is detected again, it will be recreated, and any alerts that have been defined will fire again.

Automatically Perform an OS Scan Rogue Devices

The recommended setting is Yes

When enabled, RAPIDS will automatically perform an OS scan of devices with an IP address. The scans take approximately one minute per IP address. Do not enable this option if your wired security team has concerns about running port scans on clients.

Filter Rogues Discovered by Remote APs

This is an Aruba-specific feature designed to ignore devices heard by Remote APs. Remote APs are often installed at home of an employee. The recommended setting is **Yes**. The corporate security team has no ability to make any

changes to neighboring devices and there are no corporate wired ports that need to be monitored.

Wired-to-Wireless Time Correlation Window

Use this option to specify a time frame for wired and wireless correlation. The recommended setting is 240 minutes. RAPIDS discovery events detected wirelessly and on a LAN will only match if the wireless and LAN discovery events occur during this time frame.

We recommend that this value match the polling period for bridge forwarding, which is four hours by default. With this configuration, any rogues seen on the wired and wireless network will be classified as such if the discovery event is within four hours. Users who are concerned about events where a rogue is on both the wired and wireless network might consider increasing this value.

Increasing this value might yield more classifications of wired/wireless correlation than expected. Similarly, some users might consider setting this value to match the Rogue AP Polling interval, which is 30 minutes by default.

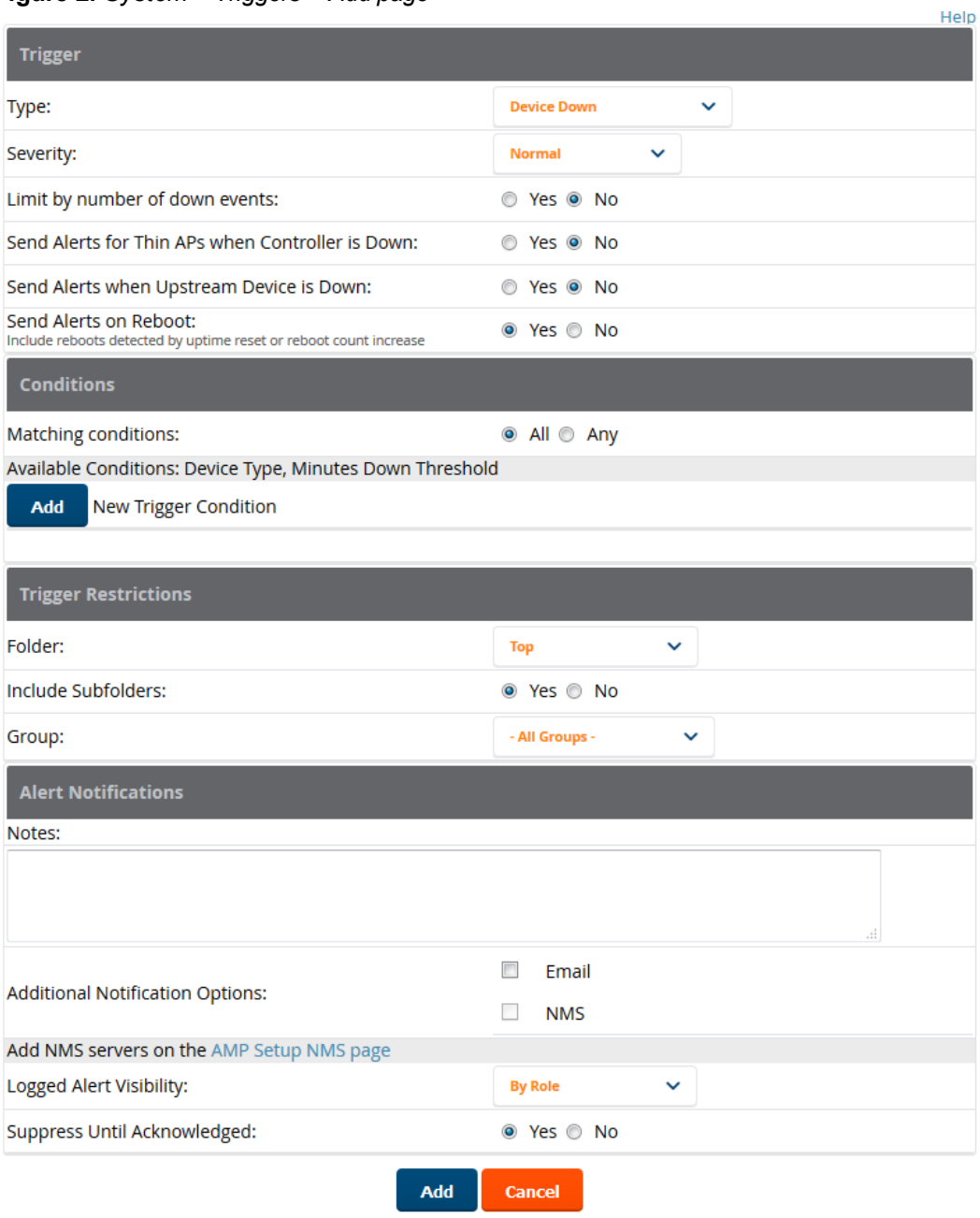
Triggers

Triggers are an important, and often overlooked, part of RAPIDS. Detecting rogue devices does not mean much if the security team is not notified about them. Triggers are defined on the **System > Triggers** page (see Figure 2). Add a Rogue Device Classified trigger type to ensure that you are notified of any rogues detected by the system. Multiple Rogue Device Classified types can be defined on one server based on the configuration of classification and threat level options. The trigger will only send an alert after a rogue device meets the conditions. The alert will not continuously sound every time the rogue device is detected.

AirWave recommends emailing the appropriate individuals when any rogue devices are classified so that the appropriate action can be taken.

Triggers must be enabled to meet PCI compliance requirements.

Figure 2: *System > Triggers > Add page*



RAPIDS has four main detection mechanisms:

- Wireless
  - Enterprise AP scans
  - AMC scans
- Wired
  - HTTP/SNMP fingerprint scans
  - Router/switch scans

Wireless Scans

Enterprise AP Scans

The first step to getting wireless discovery information is adding your supported controllers and APs into AWMS. AWMS will automatically start polling the controllers and APs via SNMP for rogue discovery information once they are monitored. The rogue data polling interval is configured on the **Groups > Basic** page under the **SNMP Polling Periods**.

Most enterprise APs support wireless scanning, but IOS APs are one notable exception. IOS APs use a proprietary protocol to transfer the rogue discovery information. AWMS can be configured to poll Wireless LAN Solution Engine (WLSE) servers for rogue discovery. See the *AirWave User Guide* for WLSE polling setup instructions.

AMC Scans

The AirWave Management Client (AMC) provides another option for customers with APs that do not report wireless discovery data or do not have full AP coverage. The AMC is a client application that runs in Windows XP. It passively listens for beaconing APs and reports them back to the RAPIDS engine via an XML interface.

Wired Scans

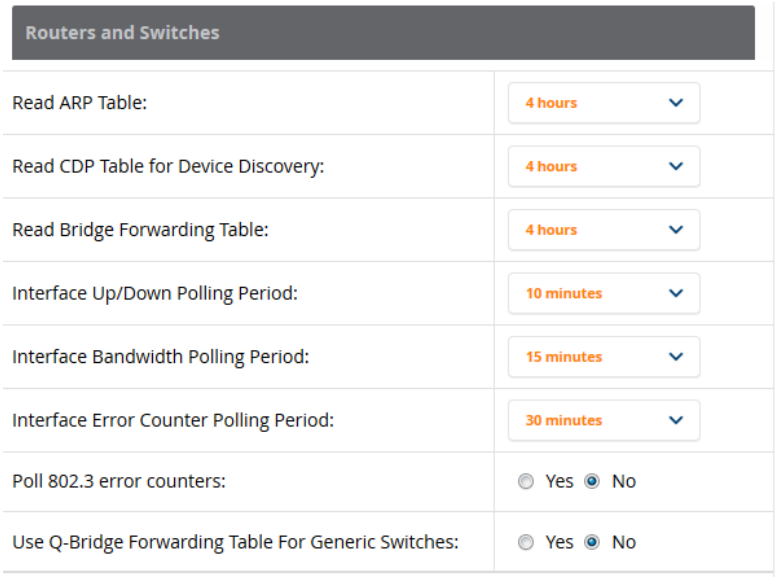
Fingerprint Scans

This section explains HTTP scans, SNMP scans and HTTP/SNMP fingerprint scans. The **Device Setup > Discover** page defines the network scans that are run. AirWave recommends running daily device discovery scans on any networks likely to have APs or rogues. The scans look at the credential challenges and rejections from the device to determine the model. The HTTP rogue scans should not have the correct rogue credentials. The HTTP scan requires that the rogue have an HTTP interface available on the scanned IP address. Similarly, the SNMP scan requires a SNMP interface on the scanned IP address. HTTP/SNMP fingerprint scans provide another valuable data point to RAPIDS. There are a number of ways a hacker can circumvent these scans but what is found is certainly a rogue worth investigating.

Polling Routers and Switches

Configuring router/switch polling is achieved by adding routers and witches to groups as monitored devices. The group has configurable wired polling periods in the **Routers and Switches** section of the **Groups > Basic** page. To view this page, navigate to **Groups > List**, select a group, then select **Groups > Basic**.(see Figure 3).

Figure 3: *Routers and Switches*

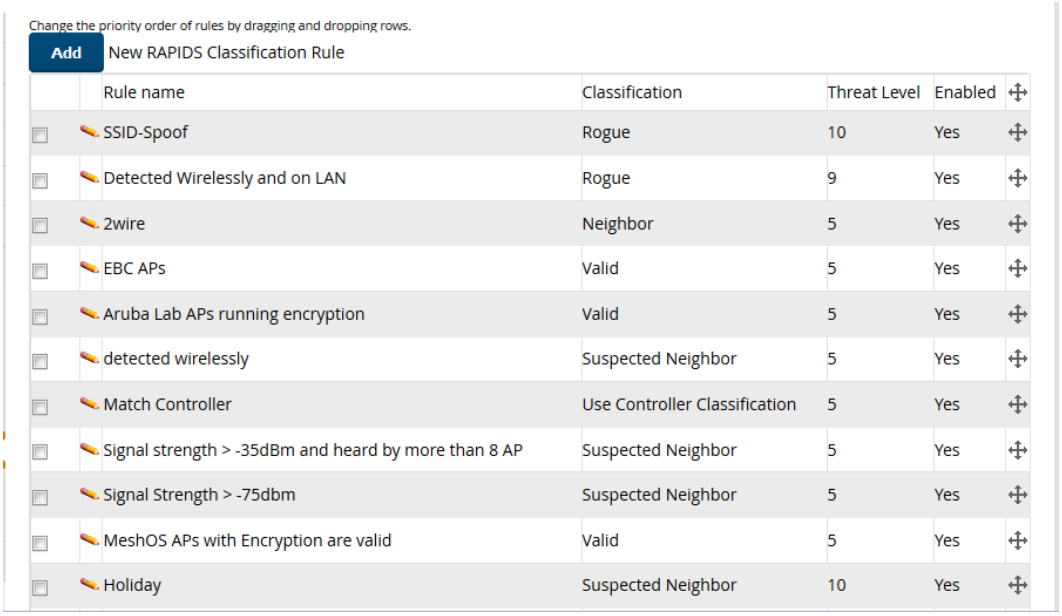


RAPIDS uses the **Read ARP Table** and the **Read Bridge Forwarding Table**. Depending on the data returned by the routers or switch, RAPIDS can gather IP addresses, LAN MAC addresses, OUI scores, LAN vendor, and switch ports. After RAPIDS has an IP address for a device, it can perform an operating system scan and discover the likeliest operating system of a device. Operating system scans can be run on demand from the **RAPIDS > Rogue APs** page using **Modify Devices,** or on the Rogue detail page.

.

The specific rules that will work best in your environment will be heavily based on your security requirements, but there are some general best practices to keep in mind. See Figure 4for an example of a typical set of rules.

Figure 4: *RAPIDS > Rules*



Rule name	Classification	Threat Level	Enabled
SSID-Spoof	Rogue	10	Yes
Detected Wirelessly and on LAN	Rogue	9	Yes
2wire	Neighbor	5	Yes
EBC APs	Valid	5	Yes
Aruba Lab APs running encryption	Valid	5	Yes
detected wirelessly	Suspected Neighbor	5	Yes
Match Controller	Use Controller Classification	5	Yes
Signal strength > -35dBm and heard by more than 8 AP	Suspected Neighbor	5	Yes
Signal Strength > -75dbm	Suspected Neighbor	5	Yes
MeshOS APs with Encryption are valid	Valid	5	Yes
Holiday	Suspected Neighbor	10	Yes

Rule Guidelines

This section contains the following topics:

Order is Important

Adding rules in the correct sequence is important because rules are implemented from the top of the list to the bottom of the list. The first rule in the list that matches will determine the classification of a device. Make sure that the most detailed rules are at the top of the list. If new information comes in and updates the device, the rule will be classified up the list of rules but not down.

Name the Rules Intuitively

Using detailed names that outline the criteria of a rule can be very helpful for locating information on the rogue list and rogue detail pages. There are a number of places where you can see the name of a classifying rule, but cannot see the detailed criteria.

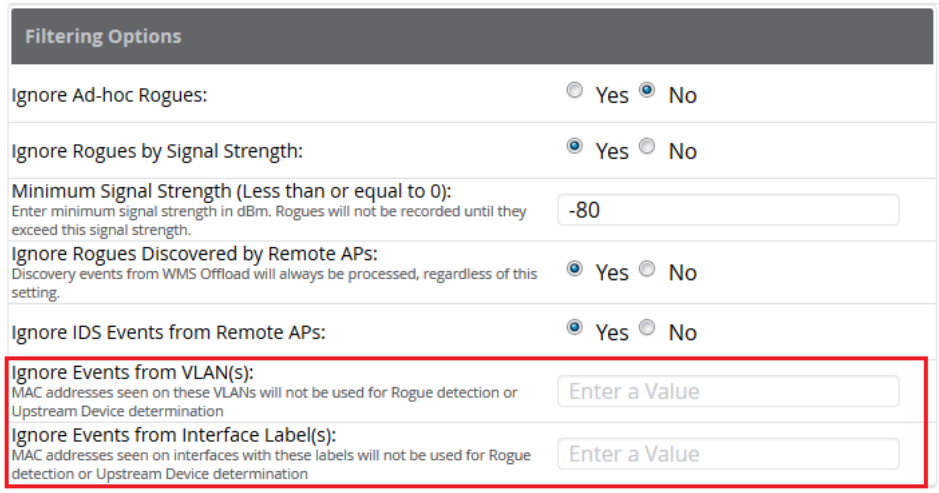
Configuring Neighbor and Valid Rules

Configuring rules that detect validity is equal in importance as configuring Rogue detection rules. Configuring Validity rules can help filter out a large number of devices that are not threats. Review the list of detected devices

and create suspect neighbor or neighbor rules based on the neighboring SSID, manufacturer, and the fact that it is not connected to the wired network.

AirWave allows you to specify VLANs and Interfaces that can be ignored in wired Rogue Discovery events and in upstream device determination. These settings, configured on the **RAPIDS > Setup** page, are particularly useful to customers who have switches in AirWave. The ports on those switches contain either special interface labels or multiple VLANs. In the case of multiple VLANs, imagine that the user has two VLANs: one acting as the corporate, and the other acting as a guest. Use the "Ignore Events from VLAN(s)" setting so that the guest VLAN wired Rogue Discovery Events can be ignored because they are not critical (see Figure 5).

Figure 5: *Ignore Events*



Protect Your SSID

Only your managed devices should be broadcasting your enterprise's SSID. Unauthorized devices broadcasting your SSID pose a significant security risk. Hackers will frequently put up rogue APs broadcasting an official SSID in an attempt to trick an unsuspecting user into associating to it. Once associated, the hacker will attempt to obtain the user's valid network credentials.

After RAPIDS identifies a rogue device, the next step is to investigate it and remove it from the network. The exact steps and workflow will depend on your organization's security standards. Some common workflows are listed below.

The last step in the workflow examples below is to delete the rogue from RAPIDS. If the rogue is rediscovered, then it will be recreated and reclassified in RAPIDS.

Occasionally, the rogue device turns out to be an approved AP that is not managed by the IT team. If that happens, update the **Notes** field with appropriate information about the rogue, and reclassify it as a valid device.

Common Rogue Response Scenarios

This section contains the following topics:

Rogue Connected to Wire

RAPIDS will report the switch and port number for devices that are discovered on the wire.

1. Review the list of switches and determine the edge switch.
2. Login to the switch and disable the port.
3. Physically trace the cable and remove the rogue device.
4. If the rogue device can be related to an employee, educate them on the dangers of rogue devices.
5. Delete the rogue from RAPIDS.

Rogues Detected Wirelessly

Wireless devices that are detected as rogues can be more difficult to track down than rogues that are detected on wired networks.

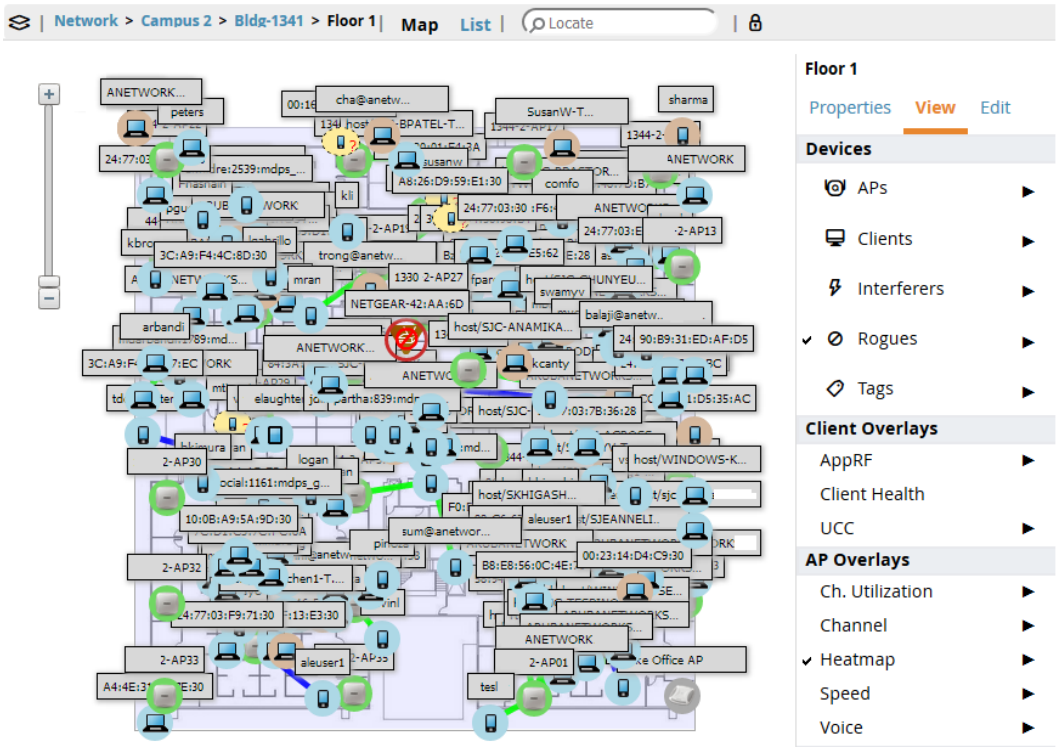
If your organization permits wireless containment, and you have devices capable of performing wireless containment, the first step is to configure the wireless containment device.

Using VisualRF to Detect a Wireless Rogue

If VisualRF is installed, locate the rogue in VisualRF.

If you are not running VisualRF or it is not up to date, navigate to the rogue detail page and investigate the list of discovering devices. Using that list of devices and discovered signal strengths, you should be able to determine the general location of the rogue device. Physically inspect the area where VisualRF has placed the rogues or where you estimate it to be.

Figure 6: *Rogues in VisualRF*



If the rogue device can be related to an employee, educate them on the dangers of rogue devices, and then delete the rogue from RAPIDS. If the rogue turns out to be a valid neighboring device, update the classification to Neighbor, acknowledge the device, and then update the Notes field with investigation information, including who located the device, when it was located, and the neighboring company that the device belongs to.

Ad-Hoc Rogues

Ad-Hoc rogues can be difficult to locate. Such rogues are highly mobile, temporary devices that are often the result of non-malicious but misconfigured laptops. Some wireless drivers will use the radio MAC address when in ad-hoc mode. It is recommended to search historical clients on AirWave for the ad-hoc MAC address. If the ad-hoc rogue is found as a client, you will know the historical users of the laptop and can contact them to properly configure the laptop. Follow the process in "Rogues Detected Wirelessly" on page 17 above if the MAC address is not found as a user.