

Summit® WM Series Rogue Access Point Detection

Overview

The Summit WM series console provides rogue Access Point (AP) detection with Summit WM Spy. It allows Altitude 350-2s to periodically scan the Radio Frequency (RF) space and report suspect devices and Peer-to-Peer networks. With this capability, Altitude 350-2s can multitask as scan devices as well as APs. This allows rogue detection to occur without installing expensive overlay sensor networks.

The Summit WM Spy feature has three components:

- RF Scanning Task
- RF Data Collector
- Analysis Engine

An RF scanning task runs on the Altitude AP. The Altitude 350 AP itself functions as a scan device. Its scan function alternates with providing its regular service for wireless clients on the network. Scan parameters are configurable in the Summit WM series controller.

The RF Data Collector (RFDC) application on the Summit WM series controller receives and manages the RF scan messages sent by the Altitude AP. The scan data includes lists of all connected Altitude 350 APs, third-party APs connected to the Summit WM controller, known friendly APs, rogue APs and ad-hoc networks. The RFDC runs on every Summit WM controller in the network.

The Analysis Engine runs on one of the Summit WM series controllers in the network. It processes the scan data from each Summit WM controller doing data collection using algorithms that make decisions about whether a detected AP is a rogue AP or not. The Analysis Engine polls all RF Data Collectors periodically and analyzes the polled data to identify any new devices. It also uses the polled data to build a summary table of APs and ad-hoc networks in the scanned area.

The Analysis Engine polls the database of known devices on the Summit WM series controller. The database contains the following information:

Altitude 350 APs registered with any Summit WM series controller in the network that has its RF Data Collector enabled and has been associated with an Analysis Engine-enabled Summit WM series controller third-party APs that have been defined and assigned to a WM-AD friendly AP—a list created in the Summit WM series controller as “friendly”.

An Altitude 350-2 is assigned to a scan group that has a particular set of scan parameters (see Figure 1). Different groups can be defined so that the administrator can assign Altitude 350-2s to logical groups to address either different geographic needs (i.e. only scan certain buildings at certain times) or coverage issues

The screenshot displays the 'Summit™ WM-Series Spy' console interface. The main window is titled 'Scan Groups' and shows configuration for a scan group named 'Group1'. The configuration includes:

- Scan Group Name: Group1
- Radio: Both
- Channel List: All
- Scan Type: Active
- Channel Dwell Time: 300 milliseconds
- Scan Time Interval: 1 (1-120) minutes
- Scan Activity: Running

Buttons for 'Start Scan', 'Stop Scan', 'Show Details', 'Run Now', 'Select All', 'Deselect All', and 'Delete this scan group' are visible. A table of 'Altitude™ APs' is shown on the right, with one AP selected. A status bar at the bottom indicates the system is running on software version V4 R1.1.11.

Figure 1: Scan Group Management Screen—an Altitude 350-2 is assigned to a scan group that has a particular set of scan parameters.

(only scan with half of the Altitude 350-2s in a given area at a given time). The algorithms and mechanisms for RF scanning have been designed to minimize the impact on user data transmission.

Altitudes can be configured to actively scan for rogues or passively listen for rogue AP beacons. Table 1 illustrates the different options.

Table 1: Active and Passive Scanning Options

	Active Altitude needs probe request, waiting for rogue and/or ad-hoc network to respond	Passive Altitude listens for rogue and/or ad-hoc networks to broadcast its beacon
User traffic enabled on a channel during scanning	Active scanning on user traffic channel only	Can receive beacons on user channel only
User traffic not enabled on any channel	Active scanning on any or all channels	Can receive beacons on any channel

Also, a GUI is provided that enables the administrator to configure the frequency at which the Altitude 350-2s within a scan group will initiate a scan (minimum one minute and maximum 120 minutes). Upon completion of the scan, Altitude 350-2 will send back the results to the Summit WM series controller and then wait for the next scan interval to repeat the process.

The Analysis Engine looks for APs based on seven conditions. If a problem is found, an event is logged and an SNMP trap is generated indicating one of the following conditions has been identified:

- Unknown AP (MAC address) with an invalid SSID—Critical Alarm
—A new device has been identified
- Unknown AP (MAC address) with a valid SSID—Critical Alarm

- A device may be trying to attract users by broadcasting a known SSID
- Known AP (MAC address) with an invalid SSID—Critical Alarm
—A rogue AP may be spoofing a known MAC address
- Known Altitude 350-2 with an invalid SSID—Major Alarm
—A rogue AP may be spoofing an Altitude 350-2 using a known MAC address
- Device that is in ad-hoc mode (IBSS)—Major Alarm
—A client configured in ad-hoc mode has been identified
- Inactive Altitude 350-2 with known SSID—Major Alarm
—A “known” Altitude 350-2 has been detected that the Summit WM series controller has identified as not in service (possibly stolen)
- Inactive Altitude 350-2 with unknown SSID—Major Alarm
—A “known” Altitude 350-2 with an unknown SSID has been detected that the Summit WM series controller has identified as not in service (possibly stolen)

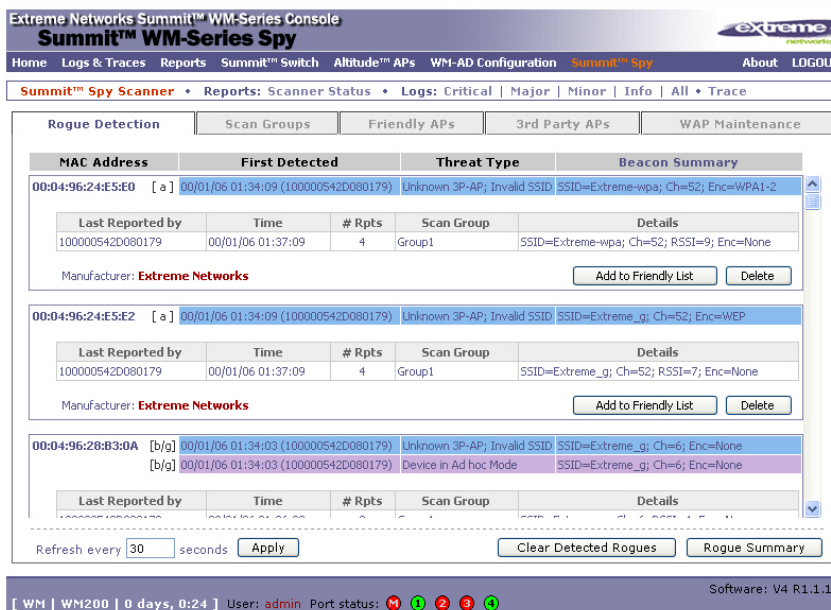


Figure 2: Rogue AP Summary Screen

With each event, the following information will be reported:

- Scanning Altitude 350-2 name and scan group
- Detection date and time
- Rogue SSID and channel
- Signal strength (RSSI)
- Security/Encoding type (eg. WEP, 802.1X, none, etc)

This information is available through SNMP, or by viewing a report screen. In addition, a summary screen is provided as a pop-up window (see Figure 3) that provides a summary of all potential problem areas on a single screen. The rogue AP alarm can be received and displayed by EPICenter, Extreme Networks unified management system.

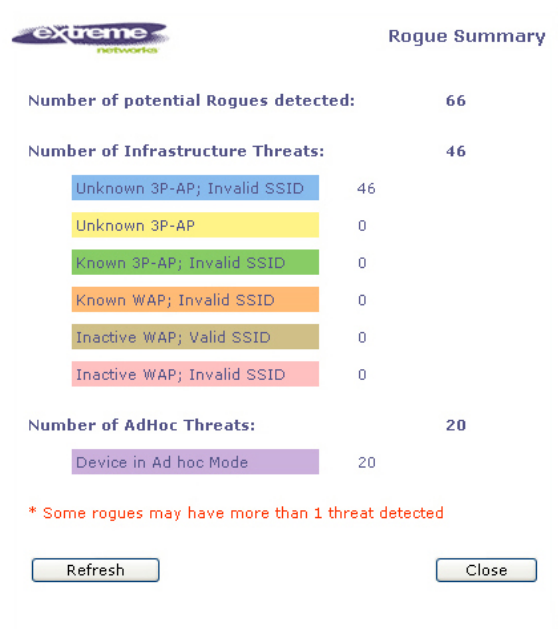


Figure 3: Rogue AP Summary Screen



www.extremenetworks.com

email: info@extremenetworks.com

Corporate and North America
 Extreme Networks, Inc.
 3585 Monroe Street
 Santa Clara, CA 95051 USA
 Phone +1 408 579 2800

Europe, Middle East, Africa and South America
 Phone +31 30 800 5100

Asia Pacific
 Phone +852 2517 1123

Japan
 Phone +81 3 5842 4011

© 2007 Extreme Networks, Inc. All rights reserved.
 Extreme Networks, the Extreme Networks Logo, and Summit are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries.
 Specifications are subject to change without notice