

# Summit® WM Support for Third-Party Access Points

## Overview

Summit WM series of WLAN controllers supports third-party Access Points (APs). This solution allows deployment of a Summit WM series controller in a way that integrates legacy third-party APs, using a combination of network routing and authentication techniques. With this solution, traffic remains local to the network to which the third-party AP is connected. The administrator can setup the policy to block all external connections and only allow traffic flows for clients to access resources on the same LAN segment. Alternatively, the third-party AP mode in the Summit WM controller can route wireless traffic to outside of firewall or provide limited network access control to the corporate networks.

## Differences between Third-Party APs and Altitude APs

The primary difference between third-party APs and Altitude APs on the Summit WM series controller is that a third-party AP exchanges data with the Summit WM series controller's data port using the standard IP over Ethernet protocol. Some other differences include:

- Third-party APs do not support the tunneling protocol for encapsulation.
- The Wireless Mobility Access Domain (WM-AD) used for third-party APs is mapped to the physical data port and the default gateway for the mobile units is mapped to the wireless mobility controller.

- Summit WM cannot directly control or manage the configuration of a third-party AP. For example, the third-party APs are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other WM-AD. Therefore, roaming from third-party APs to Altitude APs is not supported.
- Privacy (encryption) cannot be defined and provisioned on Summit WM for third-party APs. Therefore, privacy must be configured on each individual third-party AP.

## Concept

In a third-party AP setup, one of the data ports on Summit WM is defined as a third-party AP port (see Figure 1). This prepares the port to support a third-party AP setup that allows the mapping of the WM-AD to the physical port.

## Connecting Third-Party APs

The installation of a third-party AP must reside on a separate LAN segment that has Summit WM as its default gateway. Each third-party AP must have their routing capability disabled and be acting as Layer 2 bridges. The configuration of a static route should be defined in the Summit WM configuration to reach the third-party APs. This will route the third-party AP to its designated SSID/Subnet.

The screenshot displays the Summit WM Series Console interface. The main content area is titled "Management Port Settings" and shows the following configuration:

- Hostname: WM
- Domain: extremenetworks.com
- IP Address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Management Gateway: 192.168.1.2
- Primary DNS:
- Secondary DNS:

Below this, the "Interfaces" section contains a table with the following data:

Enable	Port	VLAN	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input checked="" type="checkbox"/>	esa0	U	10.10.145.3	00:04:96:34:4E:52	255.255.255.0	Router	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	U	10.0.1.1	00:04:96:34:4E:53	255.255.255.0	3rd Party	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa2	U	10.0.2.1	00:04:96:34:4E:54	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	esa3	U	10.45.201.145	00:04:96:34:4E:55	255.255.252.0	Host Port	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the table, the configuration for the selected "3rd Party" port (esa1) is shown:

- IP address: 10.0.1.1
- Subnet mask: 255.255.255.0
- VLAN ID:  Tagged - ID:   Untagged
- Function: 3rd Party AP
- MTU: 1500
- Internal VLAN ID: 1
- Multicast Support: Disabled

At the bottom of the console, a status bar indicates "Interfaces updated successfully" and shows system information: [ WM | WM200 | 0 days, 0:57 ] User: admin Port status: [ 4 icons ] Software: V4 R1.1.11

Figure 1: One of the Data Ports on Summit WM is Defined as a “Third-Party AP” Port.

## WM-AD for Third-Party APs

When configuring a WM-AD for a third-party AP, a dedicated Access Domain must be defined as a third-party AP port. The third-party AP must be defined by its IP Address and MAC address to Summit WM. It will appear in the list of APs known to the Summit WM series controller. The third-party AP WM-AD is then isolated from the rest of the WLAN network (see Figure 2).

Summit WM then assumes control over the Layer 3 functions such as DHCP. The DHCP server within the third-party AP must be disabled, so that the IP address assignment for any wireless device on the AP is from the DHCP server at Summit WM with WM-AD information. (After the third-party AP WM-AD is created, you can have internal or external DHCP server which can provide an IP addresses to Wireless Client.)

The figure consists of two screenshots of the Extreme Networks Summit WM-Series Console, showing the configuration of a 3rd Party AP.

**Top Screenshot: 3rdParty Configuration**

- Global Settings:**
  - WM Access Domains: 3rdParty (selected), EBC\_CorpAAA, EBC\_Guest, EBC\_Video, EBC\_Voice, Interop, Interop\_Inter net, Interop\_Temp\_ Access
  - Buttons: Add subnet, Rename subnet, Delete subnet
- 3rdParty Configuration:**
  - Topology: RF, Auth & Acct, RAD Policy, Filtering
  - WM-AD Mode: Routed
  - DHCP Option: Local DHCP Server
  - Gateway: 10.0.1.1
  - Mask: 255.255.255.0
  - Address Range: from 10.0.1.2 to 10.0.1.254
  - B'cast Address: 10.0.1.255
  - Domain Name:
  - Lease (seconds): default 36000, max 2592000
  - DNS Servers:
  - WINS:
  - Network Assignment: Assignment by: SSID, Use 3rd Party AP (checked)
  - Timeout: Idle (pre) 5 minutes, (post) 30 minutes, Session: 0 minutes
  - Next Hop Routing: Next Hop Address: , OSPF Route Cost: 50000, Disable OSPF Advertisement (unchecked)
  - Buttons: Save, Cancel

**Bottom Screenshot: 3rdParty Configuration**

- Global Settings:** (Same as top screenshot)
- 3rdParty Configuration:**
  - Topology: RF, Auth & Acct, RAD Policy, Filtering
  - SSID: 3rd-Party
  - 3rd Party APs:
  - IP Address: 10.0.1.15
  - MAC Address: 00:00:00:03:02:01
  - Buttons: Add, Delete, Save, Cancel

Both screenshots show the status bar at the bottom: [ WM | WM200 | 0 days, 1:02 ] User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] Software: V4 R1.1.11

Figure 2: WM-AD for Third-Party AP.

The WM-AD setting permits the definition of policy, such as Captive Portal, that manages the network access control for wireless users connected to these APs. The Captive Portal authentication uses a secure “http” page at which it can be setup with the WM-AD. The RADIUS Attributes and the Filter IDs must be defined to match those in RADIUS. The configuration of the filtering rules must be defined for the third-party APs. Since the third-party APs are mapped to a physical port, the Exception filters must on the physical port.

## Summit Spy and Third-Party APs

The third-party APs that have been defined and assigned to a WM-AD are considered as known APs by Summit Spy engines during rogue AP detection. The known third-party APs are listed separately in a screen. The third-party APs that were deleted when search engines are running are maintained as a separate list. Furthermore, the third-party AP that appears as a rogue AP can be added to the friendly AP list.

## Considerations:

- On the Summit WM data port layout (see Figure 3), only one data port can be dedicated to third-party APs.
- The third-party data port must be configured to handle third-party APs only. Any implementation of Altitude 350 APs to the same data port can result in loss of SLP Discovery to the Altitude 350 AP.
- When the third-party AP is selected on the WM-AD, by default all management by Summit WM to the AP will be turned off.
- The third-party AP must not be connected directly to a router port since the APs are connected to Summit WM as Layer 2 APs.
- Summit WM does not control the security policy on the third-party AP. If the third-party AP is not configured to use encryption, the traffic between the third-party AP and the clients are NOT encrypted.

The screenshot shows the Summit WM Series Switch console interface. The main content area is titled "Management Port Settings" and displays the following configuration:

- Hostname: WM
- Domain: extremenetworks.com
- IP Address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Management Gateway: 192.168.1.2
- Primary DNS:
- Secondary DNS:

Below this is a "Modify" button. The "Interfaces" section contains a table with the following data:

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input checked="" type="checkbox"/>	esa0	U	10.10.145.3	00:04:96:34:4E:52	255.255.255.0	Router	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	U	10.0.1.1	00:04:96:34:4E:53	255.255.255.0	3rd Party	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa2	U	10.0.2.1	00:04:96:34:4E:54	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	esa3	U	10.45.201.145	00:04:96:34:4E:55	255.255.252.0	Host Port	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the table, the configuration for the selected interface (esa1) is shown:

- IP address: 10.0.1.1
- Subnet mask: 255.255.255.0
- VLAN ID:  Tagged - ID:   Untagged
- Function: 3rd Party AP
- MTU: 1500
- Internal VLAN ID: 1
- Multicast Support: Disabled

At the bottom, there are "Save" and "Cancel" buttons. A status bar at the very bottom indicates "Interfaces updated successfully" and shows system information like "WM | WM200 | 0 days, 0:57 | User: admin | Port status: [M][1][2][3][4]" and "Software: V4 R1.1.11".

Figure 3: Summit WM Data Port Layout.



www.extremenetworks.com

email: info@extremenetworks.

**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.