

## 6 Availability, mobility, and controller functionality

This chapter describes the availability and mobility concepts, including:

- [Availability overview](#)
- [Mobility manager](#)
- [Defining management users](#)
- [Configuring network time](#)
- [Configuring Check Point event logging](#)
- [Enabling SNMP](#)
- [Using controller utilities](#)
- [Configuring Web session timeouts](#)

The Summit WM series switch provides additional functionality including:

- **Availability** – Maintains service availability in the event of a Summit WM series switch outage
- **Mobility** – Allows multiple Summit WM series switches on a network discover each other and exchange information about a client session. A maximum of up to 8 controllers can be linked to allow users to transparently roam across controllers in the mobility domain.

### Availability overview

The Summit WM series switch, access points, and WLAN switch software system provides this feature to maintain service availability in the event of a Summit WM series switch outage.

The availability feature links two Summit WM series switches as a pair, to share information about their Altitude APs. If one controller fails, its Altitude APs are allowed to connect to the backup controller. The second Summit WM series switch provides the wireless network and a pre-assigned WM Access Domain Service (WM-AD) for the Altitude AP.



#### NOTE

---

*The Summit WM series switch's mobility domain licence (MDL) limits the number of APs that are allowed to connect to the controller. During a failover event, the maximum number of failover APs a backup controller can accommodate is equal to the number of MDLs that are purchased for that system.*



#### NOTE

---

*Altitude APs that attempt to connect to a backup controller during a failover event are assigned to the WM-AD that is defined in the system's default AP configuration. If a system default AP configuration does not exist for the controller, the failover AP will not be assigned to any WM-AD.*

*Also, the default AP configuration assignment is only applicable to new APs that failover to the backup controller. Any AP that has previously failed-over and is already known to the backup system will receive the configuration already present on that system.*

*For more information, see [“Configuring the default AP settings”](#) on page 66.*

From the viewpoint of an Altitude AP, if a Summit WM series switch or the connection to it fails, the Altitude AP begins its discovery process. The Altitude AP is directed to the appropriate backup controller of the pair. This connection may require the Altitude AP to reboot. Users on the Altitude AP must log in again and be authenticated on the second Summit WM series switch.

**NOTE**

*The availability feature provides APs with a list of interfaces to which the AP should attempt to automatically connect to when a connection with an active controller link is lost. The provided list identifies the local active interfaces (enabled on the primary and backup controllers) for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority. If the active link is lost (poll failure), the AP automatically scans (pings) all addresses in its availability interface list. The AP will then connect to the highest priority interface that responds to its probe.*

## Availability prerequisites

Before you begin, ensure you have completed the following:

- Choose the primary and secondary Summit WM series switches.
- Verify the network accessibility for the TCP/IP connection between the two switches. The availability link is established as a TCP session on port 13907.
- Set up a DHCP server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both Summit WM series switches.

Now set up each Summit WM series switch separately. One method is as follows:

- 1 In the **AP Registration** screen, set up each Summit WM series switch in Stand-alone Mode and Secure Mode (allow only approved Altitude APs to connect).
- 2 In the **Topology** tab, define a WM-AD on each Summit WM series switch with the same SSID. The IP addresses must be unique. For more information, [“Topology for a WM-AD” on page 98](#). A Summit WM series switch WM200/2000 VLAN Bridged WM-AD can permit two controllers to share the same subnet (different IP addresses). This setup provides support for mobility users in a VLAN Bridged WM-AD.
- 3 On both Summit WM series switches, set the Registration Mode to Allow only approved so that no more Altitude APs can register unless they are approved by the administrator.
- 4 In the **AP Registration** screen, enable the two Summit WM series switches as an availability pair.
- 5 On each Summit WM series switch, in the **Access Approval** screen, check the status of the Altitude APs and approve any APs that should be connected to that controller.

System AP defaults can be used to assign a group of WM-ADs to the foreign APs:

- If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, it is recommended that the AP default settings match the desired WM-AD assignment for failover APs.
- AP assignment to WM-ADs according to the AP default settings can be overwritten by manually modifying the AP WM-AD assignment. (For example, select and assign each WM-AD that the AP should connect to.)
- If specific foreign APs have been assigned to a WM-AD, those specific foreign AP assignments are used.

An alternate method to setting up APs includes:

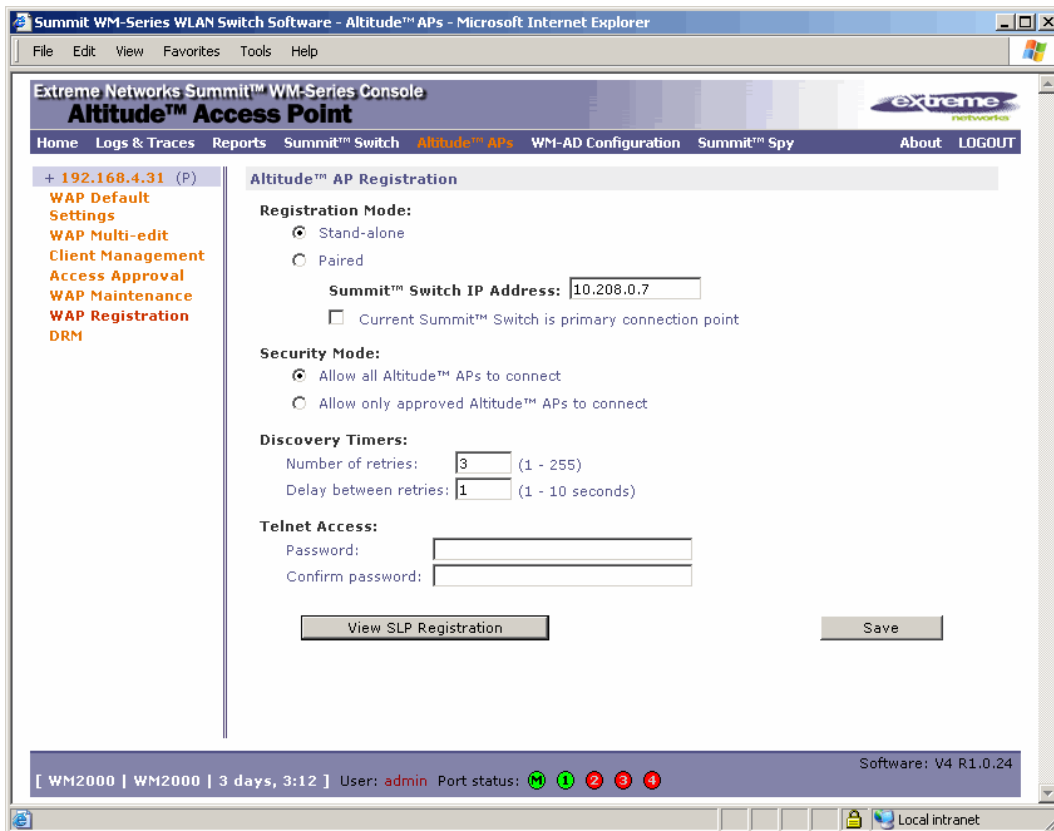
- 1 Add each Altitude AP manually to each Summit WM series switch.
  - 2 From the **AP Properties** screen, click **Add Altitude AP**.
  - 3 Define the Altitude AP and click **Add Altitude AP**.
- Manually defined APs will inherit the default AP configuration settings.

### **WARNING!**

*If two Summit WM series switches are paired and one has the Allow All option set for Altitude AP registration, all Altitude APs will register with that Summit WM series switch.*

### To set the primary or secondary Summit WM series switches for availability:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** screen is displayed.
- 2 In the left pane, click **AP Registration**. The **Altitude AP Registration** screen is displayed.



Summit WM-Series WLAN Switch Software - Altitude™ APs - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Extreme Networks Summit™ WM-Series Console  
**Altitude™ Access Point**

Home Logs & Traces Reports Summit™ Switch **Altitude™ APs** WM-AD Configuration Summit™ Spy About LOGOUT

+ 192.168.4.31 (P)  
WAP Default Settings  
WAP Multi-edit  
Client Management  
Access Approval  
WAP Maintenance  
WAP Registration  
DRM


**Altitude™ AP Registration**

**Registration Mode:**  
 Stand-alone  
 Paired  
 Summit™ Switch IP Address:   
 Current Summit™ Switch is primary connection point

**Security Mode:**  
 Allow all Altitude™ APs to connect  
 Allow only approved Altitude™ APs to connect

**Discovery Timers:**  
 Number of retries:  (1 - 255)  
 Delay between retries:  (1 - 10 seconds)

**Telnet Access:**  
 Password:   
 Confirm password:

[ WM2000 | WM2000 | 3 days, 3:12 ] User: admin Port status:  Software: V4 R1.0.24

Local intranet

- 3 To enable availability, select the **Paired** option.
- 4 Do one of the following:
  - For a primary controller, in the **Summit Switch IP Address** box, type the IP address of the physical port of the secondary Summit WM series switch. This IP address must be on a routable subnet between the two Summit WM series switches.
  - For a secondary controller, in the **Summit Switch IP Address** box, type the IP address of the Management port or physical port of the primary Summit WM series switch.

- 5 Do one of the following:
- To set this Summit WM series switch as the primary connection point, select the **Current Summit Switch is primary connect point** checkbox.
  - To set this Summit WM series switch as the secondary connection point, clear the **Current Summit Switch is primary connect point** checkbox.

If the **Current Wireless Switch is primary connect point** checkbox is selected, the specified switch waits for a request. If the **Current Wireless Switch is primary connect point** checkbox is cleared, the specified switch sends a connection request. Confirm that one switch has this checkbox selected, and the second switch has this checkbox cleared, since improper configuration of this option will result in incorrect network configuration.

- 6 To set the security mode for the Summit WM series switch, select one of the following options:
- **Allow all Altitude APs to connect** – If the Summit WM series switch does not recognize the serial number, it sends a default configuration to the Altitude AP. Or, if the Summit WM series switch recognizes the serial number, it sends the specific configuration (port and binding key) set for that Altitude AP.
  - **Allow only approved Altitude APs to connect** – If the Summit WM series switch does not recognize the serial number, the operator is prompted to create a configuration. Or, if the Summit WM series switch recognizes the serial number, it sends the configuration for that Altitude AP.

**NOTE**

*During the initial setup of the network, it is recommended to select the Allow all Altitude APs to connect option. This option is the most efficient way to get a large number of Altitude APs registered with the Summit WM series switch.*

*Once the initial setup is complete, it is recommended that the security mode is reset to the Allow only approved Altitude APs to connect option. This option ensures that no unapproved Altitude APs are allowed to connect. For more information, see [“Modifying Altitude AP settings” on page 64](#).*

- 7 To save your changes, click **Save**.

**NOTE**

*When two Summit WM series switches have been paired as described above, each Summit WM series switch's registered Altitude APs will appear as foreign on the other controller in the list of available Altitude APs when configuring a WM-AD topology.*

## Viewing the Altitude AP availability display

For more information, see [“Viewing the Altitude AP availability display” on page 193](#).

## Viewing SLP activity

In normal operations, the primary Summit WM series switch registers as an SLP service called `ac_manager`. The controller service directs the Altitude APs to the appropriate Summit WM series switch. During an outage, if the remaining Summit WM series switch is the secondary controller, It registers as the SLP service `ru_manager`.

## To view SLP activity:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** screen is displayed.
- 2 In the left pane, click **AP Registration**. The **Altitude AP Registration** screen is displayed.
- 3 To confirm SLP registration, click the **View SLP Registration** button. A pop-up screen displays the results of the diagnostic sldump tool, to confirm SLP registration.



The screenshot shows a web browser window titled "Summit™ Switch - sldump - Microsoft Internet Explorer". The page content includes the Extreme Networks logo and the title "SLP Registration". The main text displays the output of the sldump tool, starting with "Please wait while running sldump..." and ending with "Finished.". The output shows DHCP transactions for three SLP agents (10.111.0.5 and 10.111.0.6) and the results of SLPD queries for services "extreme" and "extremeNet".

```
Please wait while running sldump...

dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
ProcessSrvRplyCallback: The header functionid 2
dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
url: extreme://10.111.0.5 lifetime: 255 attributes: (attr1=ru_manager)
dhcpSendAndRecv: got 3 SLP Agents:
10.111.0.5
10.111.0.6
10.111.0.5
url: extreme://10.0.1.1 lifetime: 255 attributes: (attr1=ru_manager)
2 entries found for service "extreme".
ProcessSrvRplyCallback: The header functionid 2
0 entries found for service "extremeNet".
SLPD connection closed

Finished.
```

## Events and actions during a failover

If one of the Summit WM series switches in a pair fails, the connection between the two Summit WM series switches is lost. This triggers a failover mode condition, and a critical message is displayed in the information log of the remaining Summit WM series switch.

The screenshot shows the 'Logs & Traces' window in the Summit WM-Series Console. The window title is 'Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer'. The console header includes 'Extreme Networks Summit™ WM-Series Console' and the 'extreme networks' logo. Navigation tabs include 'Home', 'Logs & Traces', 'Reports', 'Summit™ Switch', 'Altitude™ APs', 'WM-AD Configuration', 'Summit™ Spy', 'About', and 'LOGOUT'. A breadcrumb trail shows 'SWM: Logs | Traces • WAP: Logs | Traces • Audit: GUI • DHCP: Messages'. The severity filter is set to 'Critical'. The log messages table is as follows:

Timestamp	Type	Component	Log Message
07/27/06 12:11:26	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:22	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:11:15	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:11	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:11:03	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:11:00	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:52	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:50	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:40	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:39	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:29	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:28	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:10:18	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:18	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:18	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:10:18	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493

At the bottom of the log list, it indicates '1113 critical log messages found' and 'Total pages: 2'. There are navigation buttons for 'Go' and 'Refresh', and an 'Export' button. The status bar at the bottom shows 'Software: V4 R1.0.24' and a port status indicator with four colored lights (green, red, red, red).

After the Altitude AP on the failed Summit WM series switch loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the Altitude AP is unsuccessful, it will begin the discovery process. If the Altitude AP is not successful in connecting to the Summit WM series switch after five minutes of attempting, the Altitude AP will reboot.

If the AP is assigned to different WM-ADs on the two controllers, it will reboot. Because of the pairing of the two Summit WM series switches, the Altitude AP will then register with the other Summit WM series switch.

All user sessions using the AP that fails over will terminate unless the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** screen.



### NOTE

*An Altitude AP connects first to a Summit WM series switch registered as ac\_manager and, if not found, then seeks an ru\_manager. If the primary Summit WM series switch fails, the secondary one registers as ru\_manager. This enables the secondary Summit WM series switch to be found by Altitude APs after they reboot.*

When the Altitude APs connect to the second Summit WM series switch, they will be assigned to the WM-AD that is defined in the system's default AP configuration. The wireless device users will log in again and be authenticated on the second Summit WM series switch.

When the failed Summit WM series switch recovers, each Summit WM series switch in the pair goes back to normal mode. They exchange information that includes the latest lists of registered Altitude APs. The administrator must release the Altitude APs manually on the second Summit WM series switch, so that they may re-register with their home Summit WM series switch. Foreign APs can now all be released at once by using the **Foreign** button on the Access Approval screen to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

- 1 Monitor the critical messages for the failover mode message, in the information log of the remaining Summit WM series switch (in the **Reports and Displays** section of the Summit WM series switch).
- 2 After recovery, on the Summit WM series switch that did not fail, select the foreign Altitude APs and click on the **Release** button on the **Access Approval** screen.

## Mobility manager

The Summit WM series switch, access points, and WLAN switch software system allows multiple Summit WM series switches (up to 8) on a network discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM series switches.

The solution introduces the concept of a mobility manager, where one Summit WM series switch on the network is designated as the mobility manager and all others are designated as mobility agents.

The wireless device keeps the IP address, WM-AD assignment, and filtering rules it received from its home Summit WM series switch—the Summit WM series switch that it first connected to. The WM-AD on each Summit WM series switch must have the same SSID and RF privacy parameter settings.



### NOTE

*For the mobility manager you have two options:*

- > *Rely on SLP with DHCP Option 78.*
- > *Define at the agent the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended in order to provide tighter control of the registration steps for multi-domain installations.*

The Summit WM series switch designated as the mobility manager:

- The mobility manager is explicitly identified as the manager for a specific mobility domain. Agents will connect to this manager to establish a mobility domain.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as ExtremeNet

- Defines the registration behavior for a multi-controller mobility domain set:
  - **Open mode** – A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain
  - **Secure mode** – The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents
- Establishes connection and sends a message to the mobility agent specifying the Heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent
- Sends regular Heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message

The Summit WM series switch designated as a mobility agent:

- Uses SLP or a statically configured IP address to locate the mobility manager
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager
- Updates its tables, and sets up data tunnels to and between all Summit WM series switches it has been informed of when it receives the connection-established message
- Uses the information from every Heartbeat message received to update its own tables and updates the mobility manager with information on the wireless device users and data tunnels it is managing

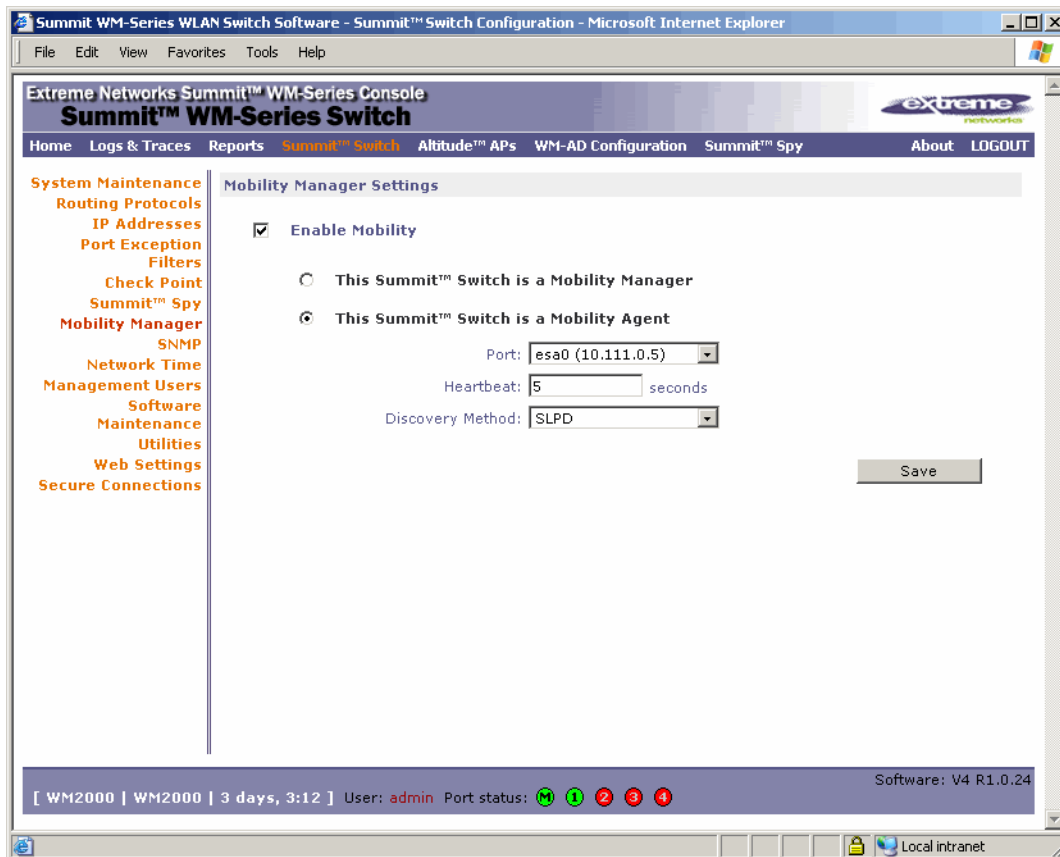
If a controller configured as the mobility manager is lost, the following occurs:

- Agent to agent connections will remain active.
- Mobility agents will continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- Participant controllers are reset to nodal operation
- Any user sessions that roamed away from their home AP are terminated and must reconnect
- Users need to reconnect to network, re-authenticate, and obtain new IP address
- The data link between active controllers remains active after the loss of a mobility manager
- Mobility agents continue to use the last set of mobility location list to service known users
- Existing users:
  - Existing users remain in mobility scenario, and if the users are known to mobility domain, they continue to be able to roam between connected controllers
- New users:
  - New users become local at attaching controller
  - Roaming to another controller resets session



## To designate a mobility manager:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.



- 3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options appear.
- 4 Select the **This Summit Switch is a Mobility Manager** option. The mobility manager options appear.
- 5 In the **Port** drop-down list, select the interface on the Summit WM series switch to be used for the mobility manager process. Ensure that the selected interface is routable on the network.
- 6 In the **Heartbeat** box, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent. The default is 5 seconds.
- 7 In the **SLP Registration** drop-down list, select whether to enable or disable SLP registration.
- 8 In the **Permission** list, select the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.

You can also add or delete controllers that you want to be part of the mobility domain. To add a controller, type the agent IP address in the box, and then click **Add**. To delete a controller, select the controller in the list, and then click **Delete**.

9 Select the Security Mode option:

- **Allow all mobility agents to connect** – All mobility agents can connect to the mobility manager.
- **Allow only approved mobility agents to connect** – Only approved mobility agents can connect to the mobility manager.

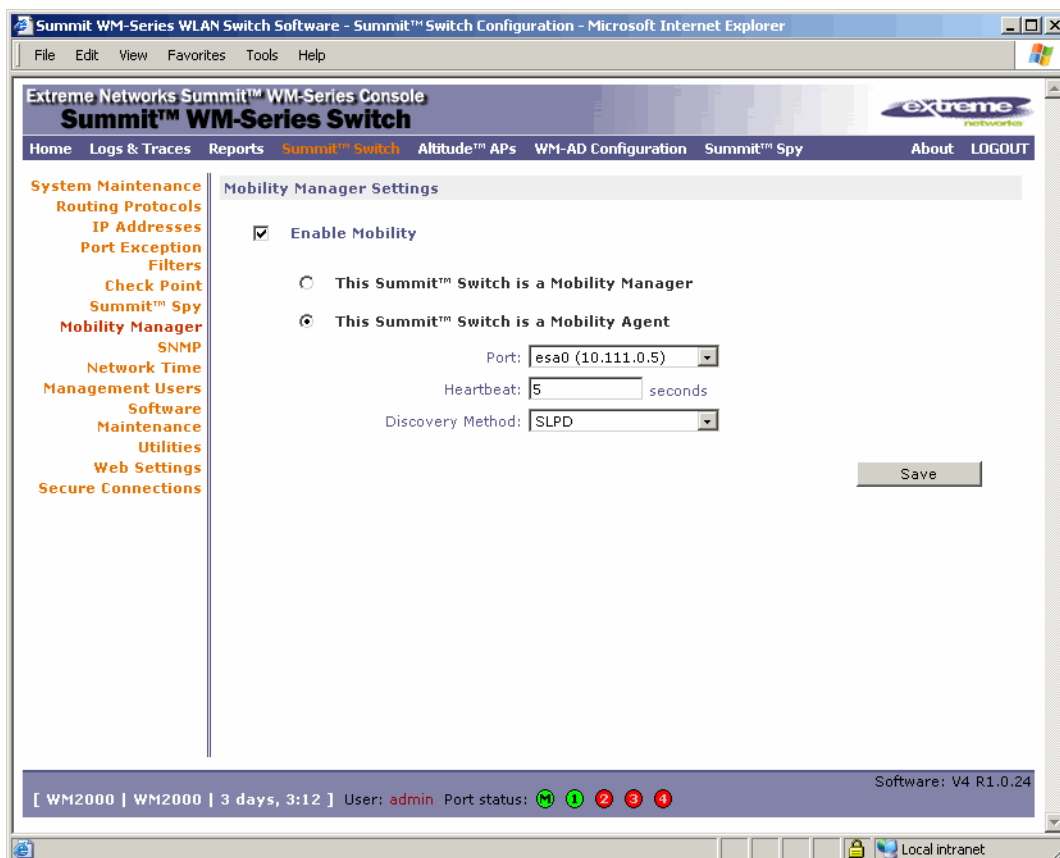
10 To save your changes, click **Save**.



*If you set up one Summit WM series switch on the network as a mobility manager, all other Summit WM series switches must be set up as mobility agents.*

## To designate a mobility agent:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** screen is displayed.
- 3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options appear,
- 4 Select the **This Summit Switch is a Mobility Agent** option. The mobility agent options appear.



- 5 In the **Port** drop-down list, select the port on the Summit WM series switch to be used for the mobility agent process. Ensure that the port selected is routable on the network.
- 6 In the **Heartbeat** box, type the time interval (in seconds) to wait for a connection establishment response before trying again. The default is **60** seconds.

- 7 From the **Discovery Method** drop-down list, select one of the following:
  - **SLPD** – Service Location Protocol Daemon is a background process acting as a SLP server. It provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to support the discovery of extremeNET service to attempt to locate the area mobility manager controller.
  - **Static Configuration** – Select Static Configuration if you want to enter the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.
- 8 In the **Mobility Manager Address** box, type the IP address for the designated mobility manager.
- 9 To save your changes, click **Save**.

## Displays for the mobility manager

For more information, see [“Viewing displays for the mobility manager”](#) on page 196.

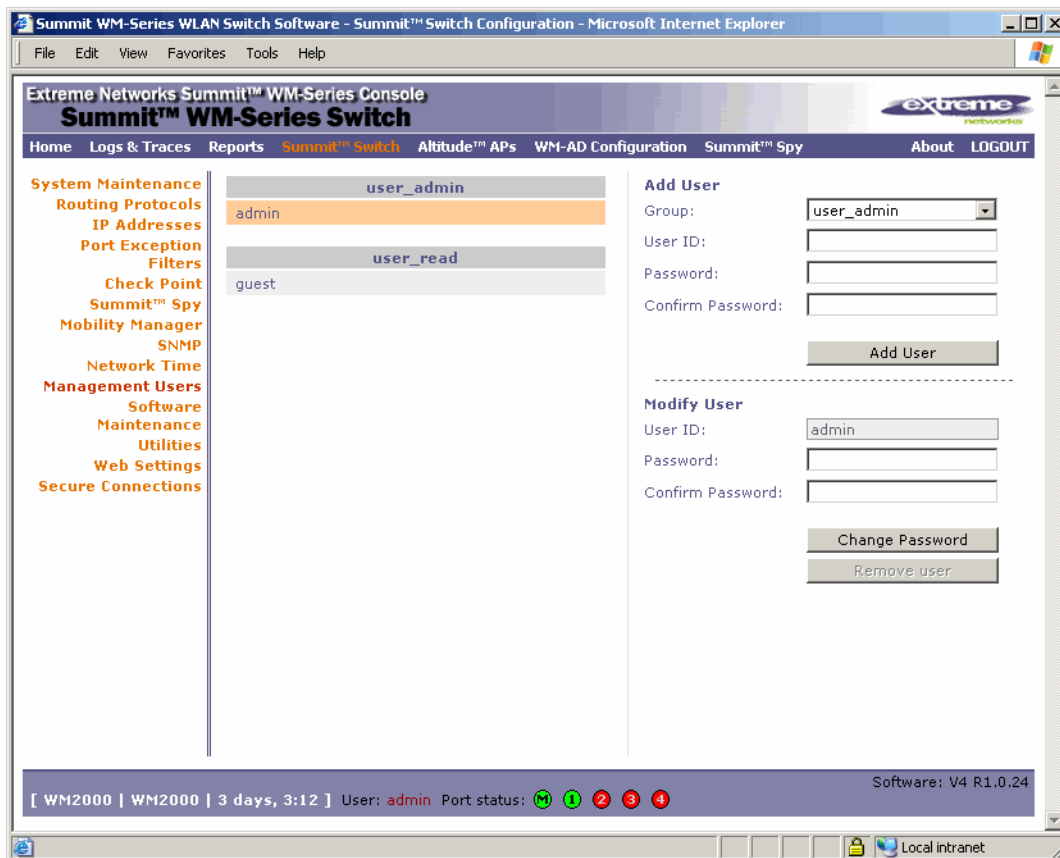
## Defining management users

In this screen you define the login user names that have access to the Summit Wireless Assistant, either for Summit WM series switch, access points, and WLAN switch software administrators with read/write privileges, or users with read only privileges. For each user added, you can also define and modify a user ID and password.

### To add a Summit WM series switch management user:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.

- In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.



The **user\_admin** list displays Admin users who have read/write privileges. The **user\_read** list is for users who have read only privileges.

- From the **Group** pull-down list, select **Admin** or **Read only**.
- In the **User ID** box, type the user ID for the new user. A User ID can only be used once, in only one category.
- In the **Password** box, type the password for the new user.
- In the **Confirm Password**, retype the password. The \$ character is not permitted.
- Click on the **Add User** button. The new user is added to the appropriate user list.

### To modify a Summit WM series switch management user:

- From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.
- To select a user to be modified, click it.
- In the **Password** box, type the new password for the user.
- In the **Confirm Password**, retype the new password.
- To change the password, click **Change Password**.

**To remove a Summit WM series switch management user:**

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click the **Management Users** option. The **Management Users** screen is displayed.
- 3 To select a user to be removed, click it.
- 4 To remove the user, click **Remove user**. The user is removed from the list.

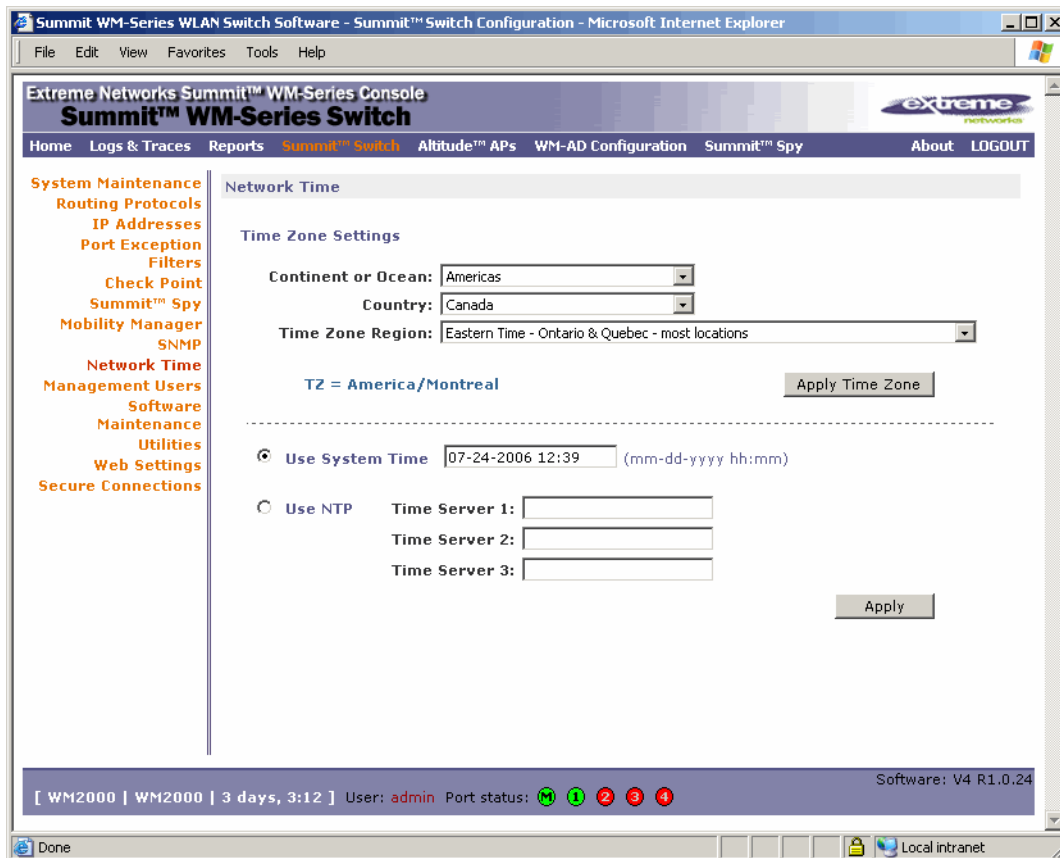
## Configuring network time

You can synchronize the elements on the network to a universal clock. This ensures accuracy in usage logs. Network time is synchronized in one of two ways:

- using system time
- using Network Time Protocol (NTP), an Internet standard protocol that synchronizes client workstation clocks.

## To apply time zone settings:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Network Time**. The **Network Time** screen is displayed.



- 3 From the **Continent or Ocean** drop-down list, select the appropriate large-scale geographic grouping for the time zone.
- 4 From the **Country** drop-down list, select the appropriate country for the time zone. The contents of the drop-down list change based on the selection in the **Continent or Ocean** drop-down list.
- 5 From the **Time Zone Region** drop-down list, select the appropriate time zone region for the selected country.
- 6 To apply your changes, click **Apply Time Zone**.

## To set system time parameters:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Network Time**. The **Network Time** screen is displayed.
- 3 To use system time, select the **Use System Time** radio button.
- 4 Type the time setting in the **Use System Time** box, using the mm-dd-yyyy hh:mm format.
- 5 To apply your changes, click **Apply**.

### To set Network Time Protocol:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Network Time**. The **Network Time** screen is displayed.
- 3 To use Network Time Protocol, select the **Use NTP** radio button.
- 4 In the **Use System Time** box, type the time setting using the mm-dd-yyyy hh:mm format.
- 5 In the **Time Server 1** box, type the IP address or FQDN of a standard NTP Time Server. You can repeat this step for the **Time Server 2** and **Time Server 3** boxes.
- 6 To apply your changes, click **Apply**.

## Configuring Check Point event logging

The Summit WM series switch can forward specified event messages to an ELA server using the OPSEC ELA protocol - Event Logging API (Application Program Interface). On the ELA server, the event messages are tracked and analyzed, so suspicious messages can be forwarded to a firewall application that can take corrective action.

Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for inter operability.

When ELA is enabled on the Summit WM series switch, it forwards the specified event messages from its internal event server to the designated ELA Management Station on the enterprise network.



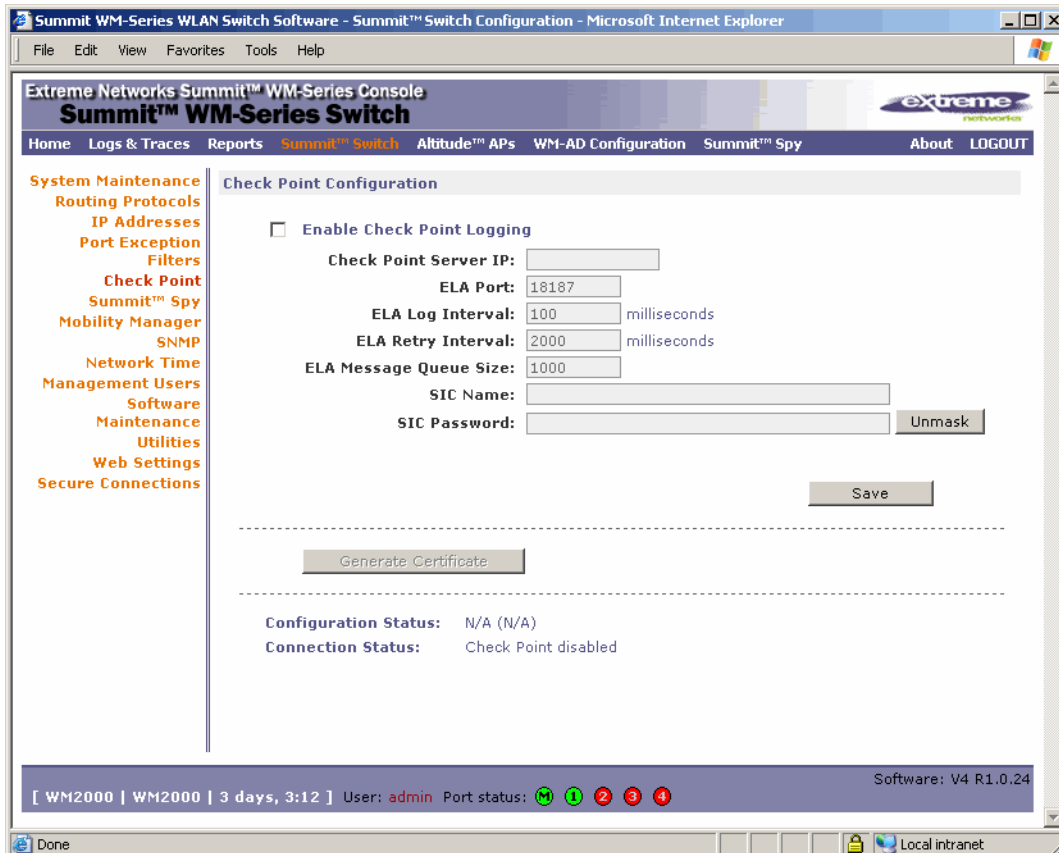
#### NOTE

---

*Before you set up the Summit WM series switch, you must first create OPSEC objects for Summit WM series switch in the Check Point management software. The name and password you define must also be entered into the Summit WM series switch Check Point configuration screen.*

## To enable and configure Check Point:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Check Point**. The **Check Point Configuration** screen is displayed.



- 3 To enable check point logging, select the **Enable Check Point Logging** checkbox.
- 4 Type the following information:
  - **Check Point Server IP** – Specifies the IP address of the ELA Management Station
  - **ELA Port** – Specifies the port to use for ELA. The default port is 18187.
  - **ELA Log Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting to log once there is a connection between Summit WM series switch and the Check Point gateway. The default is **100** milliseconds.
  - **ELA Retry Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting a re-connection between Summit WM series switch and the Check Point gateway. The default is **2000** milliseconds.
  - **ELA Message Queue Size** – Specifies the number of messages the log queue holds if the Summit WM series switch and the Check Point gateway become disconnected. The default is **1000** log entries.
  - **SIC Name** – Specifies the Secure Internal Communication (SIC) Name, your security-based ID.
  - **SIC Password** – Specifies your Secure Internal Communication (SIC) password. You can use the **Unmask** button to display the password.
- 5 To save your changes, click **Save**.



- 6 To create the certificate to be sent to the ELA Management Station, click **Generate Certificate** button. If the certificate is properly generated and the connection with the ELA Management Station is made, the **Connection Status** section displays the following message:

OPSEC Connection OK

If there is an error in generating the certificate or establishing the connection, the **Connection Status** section displays the following message:

OPSEC Connection Error

## ELA Management Station events

The events for the ELA Management Station are grouped under Extreme Networks and are mapped as info events and alert events. The alerts include:

- Altitude AP registration and/or authentication failed
- Authentication User Request unsuccessful
- RADIUS server rejected login (Access Rejected)
- An unknown AP has attempted to connect. AP authentication failure.
- A connection request failed to authenticate with the CM messaging server. This may indicate port-scanning of the Summit WM series switch, or a back-door access attempt.
- Unauthorized client attempting to connect

## Enabling SNMP

The Summit WM series switch, access points, and WLAN switch software system supports Simple Network Management Protocol (SNMP), Version 1 and 2c. SNMP, a set of protocols for managing complex networks, is used to retrieve Summit WM series switch statistics and configuration information.

SNMP sends messages, called protocol data units (PDUs), to different parts of a network. Devices on the network that are SNMP-compliant, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

## MIB support

The Summit WM series switch, access points, and WLAN switch software system accepts SNMP Get commands and generates Trap messages. Support is provided for the retrieval information from the router MIB-II (SNMP\_GET) as well as SNMP traps. The supported MIBs include:

- SNMPv2-MIB
- IF-MIB
- IEEE802dot11-MIB
- RFC1213-MIB



### NOTE

*The Summit WM series switch is not fully compliant with MIB II. For example, esa/IXP ports only provide interface statistics.*

The Extreme Networks **Enterprise MIB** includes:

- EXTREME-SUMMIT-WM-MIB.my
- EXTREME-SUMMIT-WM-SMI
- EXTREME-SUMMIT-DOT11-EXTNS-MIB
- EXTREME-SUMMIT-WM-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

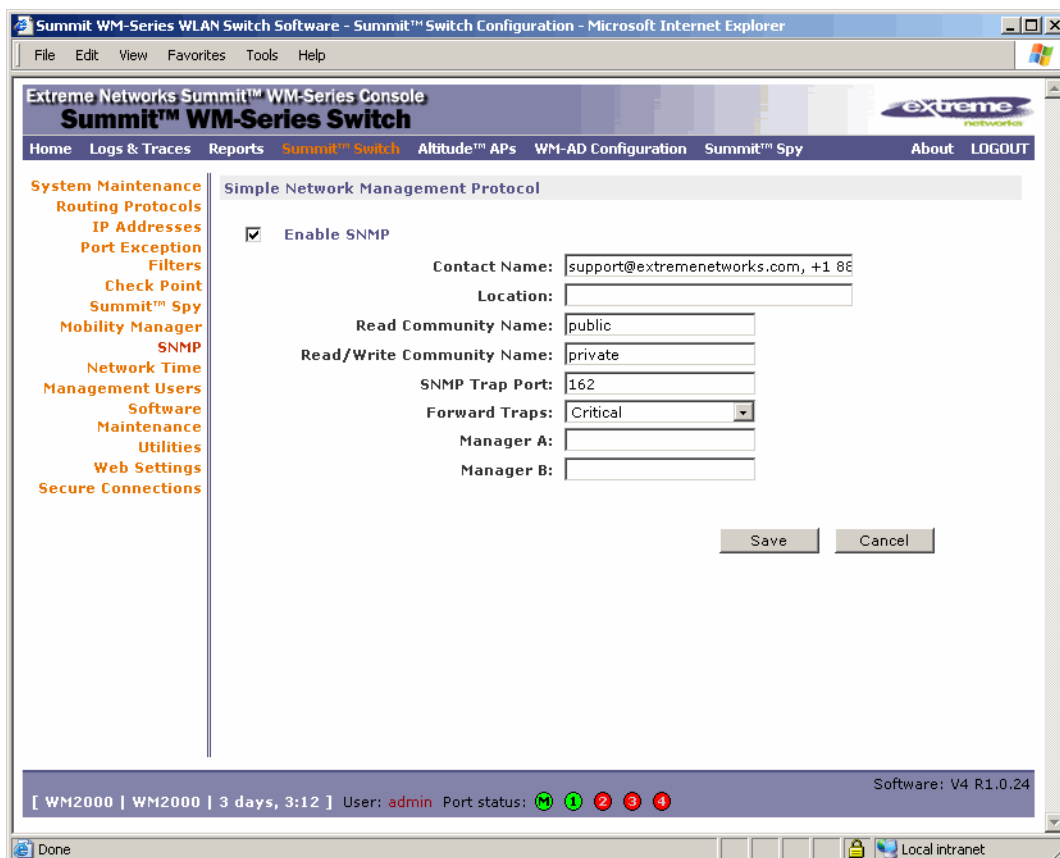
The Summit WM series switch is the only point of SNMP access for the entire system. In effect, the Summit WM series switch proxies sets, gets, and alarms from the associated Altitude APs.

## Enabling SNMP on the Summit WM series switch

You can enable SNMP on the Summit WM series switch to retrieve statistics and configuration information.

### To enable SNMP Parameters:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **SNMP**. The **Simple Network Management Protocol** screen is displayed.



3 Type: the following information:

- **Contact Name** – Specifies the name of SNMP administrator.
- **Location** – Specifies the location of the SNMP administration machine.
- **Read Community Name** – Specifies the community name for users with read privileges.
- **Read/Write Community Name** – Specifies the community name for users with read and write privileges.
- **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.
- **Forward Traps** – Specifies the security level of the traps to be forwarded. From the drop-down list, select **Informational**, **Minor**, **Major**, or **Critical**.
- **Manager A** – Specifies the IP address of the specific machine on the network where the SNMP traps are monitored.
- **Manager B** – Specifies the IP address of a second machine on the network where the SNMP traps are monitored, if Manager A is not available.



#### NOTE

*For security purposes, it is recommended that you immediately change the Read Community Name (public) and the Read/Write Community Name (private) to names that are less obvious and more secure.*

## Using controller utilities

You can use Summit WM series switch utilities to test a connection to the target IP address or to record the route through the Internet between your computer and the target IP address.

### To test or record IP address connections:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Utilities**. The **Summit Switch Utilities** screen is displayed.
- 3 In the **Target IP Address** box, type the IP address of the destination computer.
- 4 To test a connection to the target IP address, click **Ping**.

- To record the route through the Internet between your computer and the target IP address, click **Trace Route**.

The following is an example of a screen after clicking the **Trace Route** button.

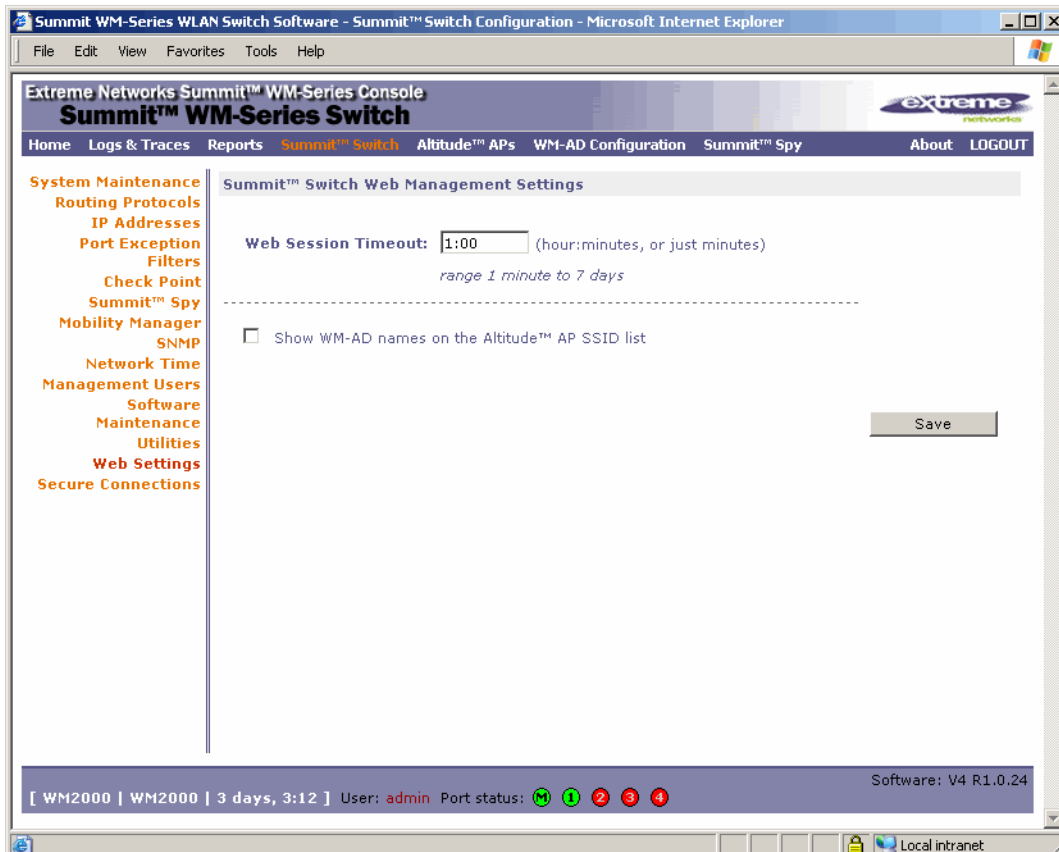


## Configuring Web session timeouts

You can configure the time period to allow Web sessions to remain inactive before timing out.

## To configure Web session timeouts:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Web Settings**. The **Summit Switch Web Management Settings** screen is displayed.



- 3 In the **Web Session Timeout** box, type the time period to allow the Web session to remain inactive before it times out. This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.
- 4 Select the **Show WM-AD names on the Altitude AP SSID list** checkbox to allow the names of the WM-ADs to appear in the SSID list for Altitude APs.
- 5 To save your settings, click **Save**.

### NOTE

Screens that auto-refresh will time out, unless a manual action takes place prior to the end of the timeout period.



## 7

## Working with third-party APs

You can set up the Summit WM series switch to handle wireless device traffic from third-party access points, providing the same policy and network access control. This process requires the following steps:

- Step 1 – Define a data port as a third party AP port:
- Step 2 – Define a WM-AD for the third-party AP port:
- Step 3 – Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD:
- Step 4 – Define filtering rules for the third-party APs:

To set up third-party APs:

### Step 1 – Define a data port as a third party AP port:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **IP Address**. The **Management Port Settings and Interfaces** screen is displayed.

The screenshot shows the Summit WM-Series Switch configuration interface. The left pane is expanded to 'IP Address'. The main area displays 'Management Port Settings' and 'Interfaces'.

**Management Port Settings:**

- Hostname: c2000
- Domain:
- IP Address: 192.168.4.204
- Subnet mask: 255.255.255.0
- Management Gateway:
- Primary DNS:
- Secondary DNS:

**Interfaces:**

Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mgmt	SLP
<input checked="" type="checkbox"/>	esa0	U	10.206.1.17	08:00:06:81:C2:9D	255.255.255.0	Router	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	esa1	U	10.0.1.1	08:00:06:81:C2:9E	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa2	U	10.206.0.19	08:00:06:81:C2:9F	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	esa3	U	10.0.3.1	08:00:06:81:C2:A0	255.255.255.0	Host Port	1500	<input type="checkbox"/>	<input type="checkbox"/>

**Configuration details for selected port (esa0):**

- IP address: 10.206.1.17
- Subnet mask: 255.255.255.0
- VLAN ID:  Tagged - ID:
- Function: Host Port (dropdown menu showing options: Host Port, 3rd Party AP, Router)
- MTU:
- Untagged:
- Internal VLAN ID:  Multicast Support: Disabled (dropdown menu)

Buttons: Modify, Save, Cancel

Footer: [ WM2000 | WM2000 | 3 days, 3:12 ] User: admin Port status: [ M ] [ 1 ] [ 2 ] [ 3 ] [ 4 ] Software: V4 R1.0.24

- 3 Highlight the appropriate port, and in the **Function** box, select **3rd-party AP** from the drop-down list. Make sure that Management Traffic and SLP are disabled for this port.

- 4 Connect the third-party access point to this port, via a switch.

## Step 2 – Define a WM-AD for the third-party AP port:

- 1 From the main menu, click **WM-AD Configuration**. The WM-AD Configuration screen is displayed.
- 2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box, and then click **Add subnet**. The name is displayed in the **WM Access Domains** list. The **Topology** tab is displayed.

- 3 In the **Assignment by** drop-down list, click **SSID**.
- 4 To define a WM-AD for a third-party AP, select the **Use 3rd Party AP** checkbox.
- 5 Continue configuring your WM-AD as described in “[Configuring topology for a WM-AD for Captive Portal](#)” on page 98.

### NOTE

*Bridge Traffic at AP and MAC-based authentication are not available for Third Party WM-ADs.*

## Step 3 – Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD:

- 1 Click the **Auth & Acct** tab.
- 2 In the **Authentication Configuration** screen, click **Configure Captive Portal Settings**.



- 3 In the **Captive Portal Settings** screen, define the Captive Portal configuration.
- 4 Click the **RAD Policy** tab.
- 5 Define the filter IDs to match those in RADIUS server.

#### **Step 4 – Define filtering rules for the third-party APs:**

- 1 Because the third-party APs are mapped to a physical port, you must define the Exception filters on the physical port, using the Port Exception Filters screen. For more information, see [“Configuring filtering rules for a WM-AD” on page 123](#).
- 2 Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, Telnet, SNMP.

In addition, modify the following functions on the third-party access point:

- Disable the access point's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the Summit WM series switch with WM-AD information.
- Disable the third-party access point's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

Here are the differences between third-party access points and Altitude APs on the Summit WM series switch, access points, and WLAN switch software system:

- A third-party access point exchanges data with the Summit WM series switch's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party access points, the WM-AD is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A Summit WM series switch cannot directly control or manage the configuration of a third-party access point.
- Third-party access points are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other WM-AD.
- Roaming from third-party access points to Altitude APs and vice versa is not supported.



This chapter describes Summit spy concepts, including:

- [Summit spy overview](#)
- [Enabling the Analysis and data collector engines](#)
- [Running Summit Spy scans](#)
- [Analysis engine overview](#)
- [Working with Summit spy scan results](#)
- [Working with friendly APs](#)
- [Viewing the Summit spy list of third-party APs](#)
- [Maintaining the Summit spy list of APs](#)
- [Viewing the Scanner Status report](#)

## Summit spy overview

The Summit spy is a mechanism that assists in the detection of rogue APs. Summit spy functionality does the following:

### Altitude AP:

- Runs a radio frequency (RF) scanning task.
- Alternating between scan functions, providing its regular service to the wireless devices on the network.

### Summit WM series switch:

- Runs a data collector application that receives and manages the RF scan messages sent by the Altitude AP. RF data collector data includes lists of all connected Altitude APs, third-party APs, and the RF scan information that has been collected from the Altitude APs selected to perform the scan.
- Runs an Analysis Engine that processes the scan data from the data collector through algorithms that make decisions about whether any of the detected APs or clients are rogue APs or are running in an unsecure environment (for example, ad-hoc mode).



#### NOTE

---

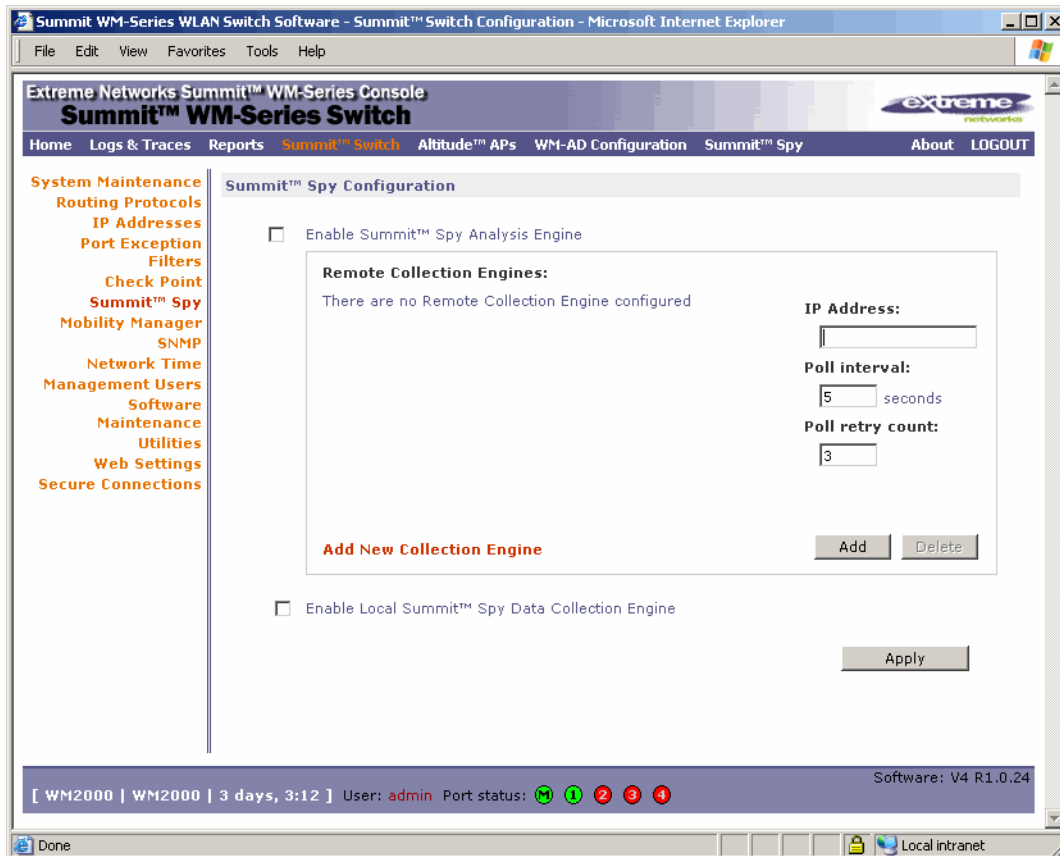
*In a network with more than one Summit WM series switch, it is not necessary for the data collector to be running on the same controller as the Analysis Engine. One controller can be a dedicated Analysis Engine while the other controllers run data collector functionality. No more than one Analysis Engine can be running at a time. You must ensure that the controllers are all routable.*

## Enabling the Analysis and data collector engines

Before using the Summit spy, you must enable and define the Analysis and data collector engines.

### To enable the Analysis engine:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 In the left pane, click **Summit Spy**. The **Summit Spy Configuration** screen is displayed.



- 3 To enable the Summit Spy Analysis Engine, select the **Enable Summit Spy Analysis Engine** checkbox.
- 4 To enable the Summit Spy Data Collection Engine on this Summit WM series switch, select the **Enable Local Summit Spy Data Collection Engine** checkbox.
- 5 To identify the remote RF Data Collector Engine that the Analysis Engine will poll for data, type the IP address of the Summit WM series switch on which the remote Data Collector resides in the **IP Address** box.
- 6 For the data collection engine:
  - In the **Poll interval** box, type (in seconds) the interval that the Analysis Engine will poll the RF Data Collector to maintain connection status. The default is 30 seconds.
  - In the **Poll retry count** box, type the number of times the Analysis Engine will attempt to poll the RF Data Collector to maintain connection status, before it stops sending requests. The default is 2 attempts.

- 7 Click **Add**. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters is displayed in the list.

**NOTE**

---

*For each remote RF Data Collection Engine defined here, you must:*

*> Enable it by selecting the Enable Summit Spy Analysis Engine checkbox on the remote Summit WM series switch*

*> Ensure that the controllers are routable by whatever means you use (for example, static routes, or OSPF).*

- 8 To add a new collection engine, click **Add Collection Engine**.
- 9 Repeat steps 4 to 7.
- 10 To save your changes, click **Apply**.

## Running Summit Spy scans

The Summit Spy feature allows you to view the following:

- Scan Groups
- Friendly APs
- Third-party APs
- AP Maintenance

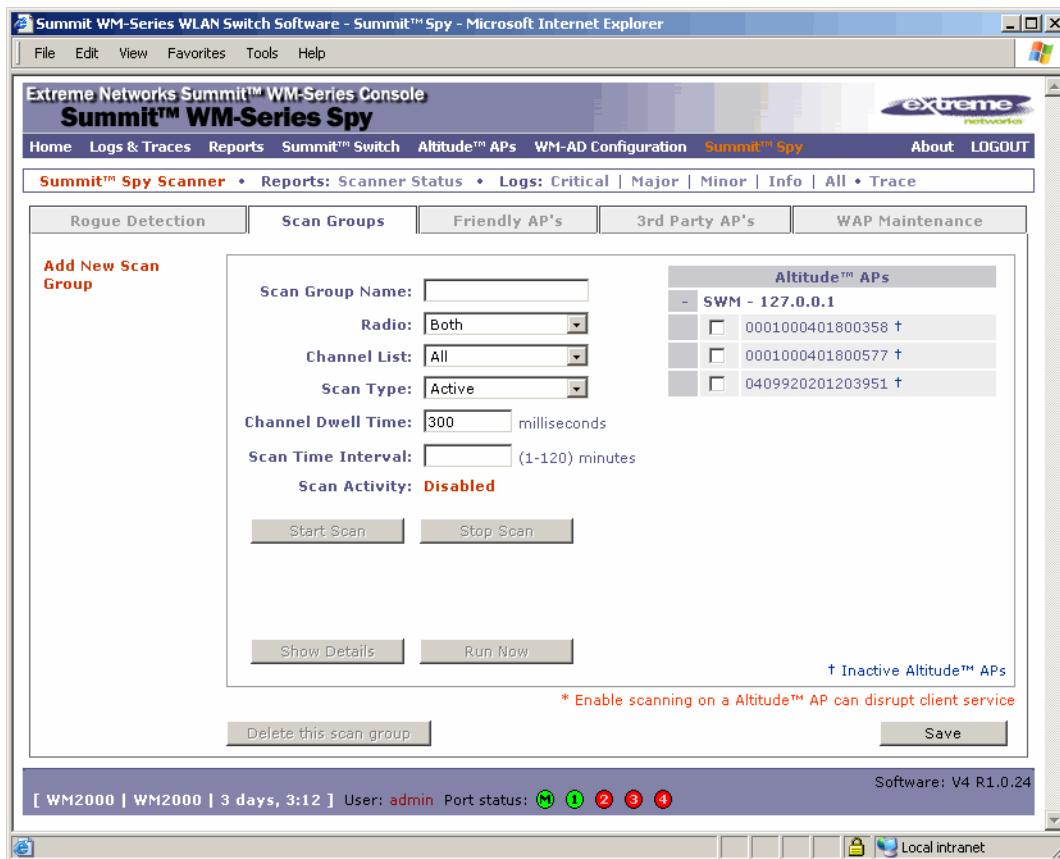
**NOTE**

---

*A scan will not run on an inactive AP, even though it is displayed as part of the Scan Group. If it becomes active, it will be sent a scan request during the next periodic scan.*

## To run the Summit Spy scan task mechanism:

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Scan Groups** tab.



- 3 In the **Scan Group Name** box, type a unique name for this scan group.
- 4 In the **Altitude APs** list, select the checkbox corresponding to the Altitude APs you want included in the new scan group, which will perform the scan function.

### NOTE

*An Altitude AP can participate in only one Scan Group at a time. It is recommended that the Scan Groups represent geographical groupings of Altitude APs.*

- 5 In the **Radio** drop-down list, select one of the following:
  - **Both** – The a and b/g radios both perform the scan function.
  - **a** – Only the a radio performs the scan function.
  - **b/g** – Only the b/g radio performs the scan function.
- 6 In the **Channel List** drop-down list, select one of the following:
  - **All** – Scanning is performed on all channels.
  - **Current** – Scanning is performed on only the current channel.
- 7 In the **Scan Type** drop-down list, select one of the following:
  - **Active** – The Altitude AP sends out ProbeRequests and waits for ProbeResponse messages from any access points.

- **Passive** – The Altitude AP listens for 802.11 beacons.
- 8 In the **Channel Dwell Time** box, type the time (in milliseconds) for the scanner to wait for a response from either 802.11 beacons in passive scanning, or ProbeResponse in active scanning.
  - 9 In the **Scan Time Interval** box, type the time (in minutes) to define the frequency at which an Altitude AP within the Scan Group will initiate a scan of the RF space. The range is from one minute to 120 minutes.
  - 10 To initiate a scan using the periodic scanning parameters defined above, click **Start Scan**.
  - 11 To initiate an immediate scan that will run only once, click **Run Now**.

**NOTE**

*If necessary, you can stop a scan by clicking Stop Scan. A scan must be stopped before modifying any parameters of the Scan Group, or before adding or removing an Altitude AP from a Scan Group.*

- 12 The **Scan Activity** box displays the current state of the scan engine.
- 13 To view a pop-up report showing the timeline of scan activity and scan results, click **Show Details**.
- 14 To save your changes, click **Save**.

## Analysis engine overview

The Analysis engine relies on a database of known devices on the Summit WM series switch, access points, and WLAN switch software system. The Analysis engine compares the data from the RF Data Collector with the database of known devices.

This database includes the following:

- **Altitude APs** – Registered with any Summit WM series switch with its RF Data Collector enabled and associated with the Analysis Engine on this Summit WM series switch.
- **Third-party APs** – Defined and assigned to a WM-AD.
- **Friendly APs** – A list created in the Summit spy user interface as potential rogue access points are designated by the administrator as Friendly.
- **Wireless devices** – Registered with any Summit WM series switch that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Summit WM series switch.

The Analysis Engine looks for access points with one or more of the following conditions:

- **Unknown MAC address and unknown SSID** (critical alarm)
- **Unknown MAC, with a valid SSID** - a known SSID is being broadcast by the unknown access point (critical alarm)
- **Known MAC, with an unknown SSID** - a rogue may be spoofing a MAC address (critical alarm)
- **Inactive Altitude AP with valid SSID** (critical alarm)
- **Inactive Altitude AP with unknown SSID** (critical alarm)
- **Known Altitude AP with an unknown SSID** (major alarm)
- **In ad-hoc mode** (major alarm)

**NOTE**

In the current release, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue requires an inspection of the geographical location of its Scan Group area, where its RF activity has been found.

## Working with Summit spy scan results

When viewing the Summit spy scan results you can delete all or selected Access Points from the scan results. You can also add Access Points from the scan results to the **Friendly AP** list.

### To view Summit Spy scan results:

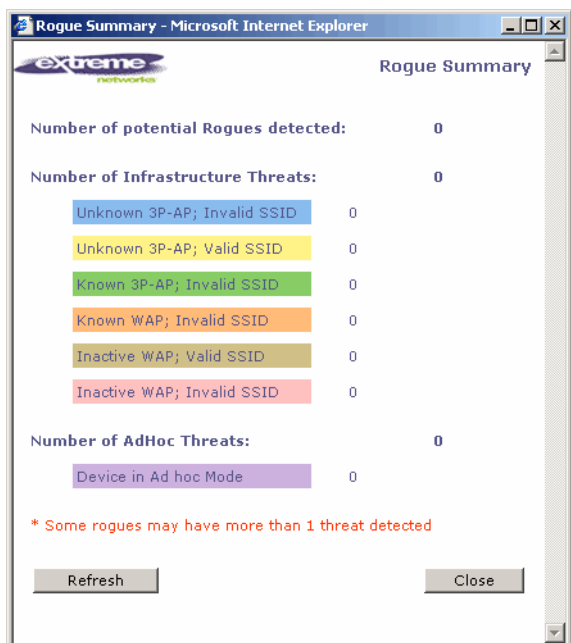
- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Rogue Detection** tab.
- 3 To modify the screen's refresh rate, type a time (in seconds) in the **Refresh every \_\_ seconds** box.
- 4 Click **Apply**. The new refresh rate is applied.



- 5 To view the Rogue Summary report, click **Rogue Summary**. The Rogue Summary report is displayed in a pop-up window.



- To clear all detected rogue devices from the list, click **Clear Detected Rogues**.

**NOTE**

To avoid the Summit spy's database becoming too large, it is recommended that you either delete Rogue APs or add them to the Friendly APs list, rather than leaving them in the Rogue list.

### To add an AP from the Summit spy scan results to the list of friendly APs:

- From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- Click the **Rogue Detection** tab.
- To add an Altitude AP to the **Friendly APs** list, click **Add to Friendly List**. The AP is removed from this list and is displayed in the **Friendly AP Definitions** section of the **Friendly AP's** tab.

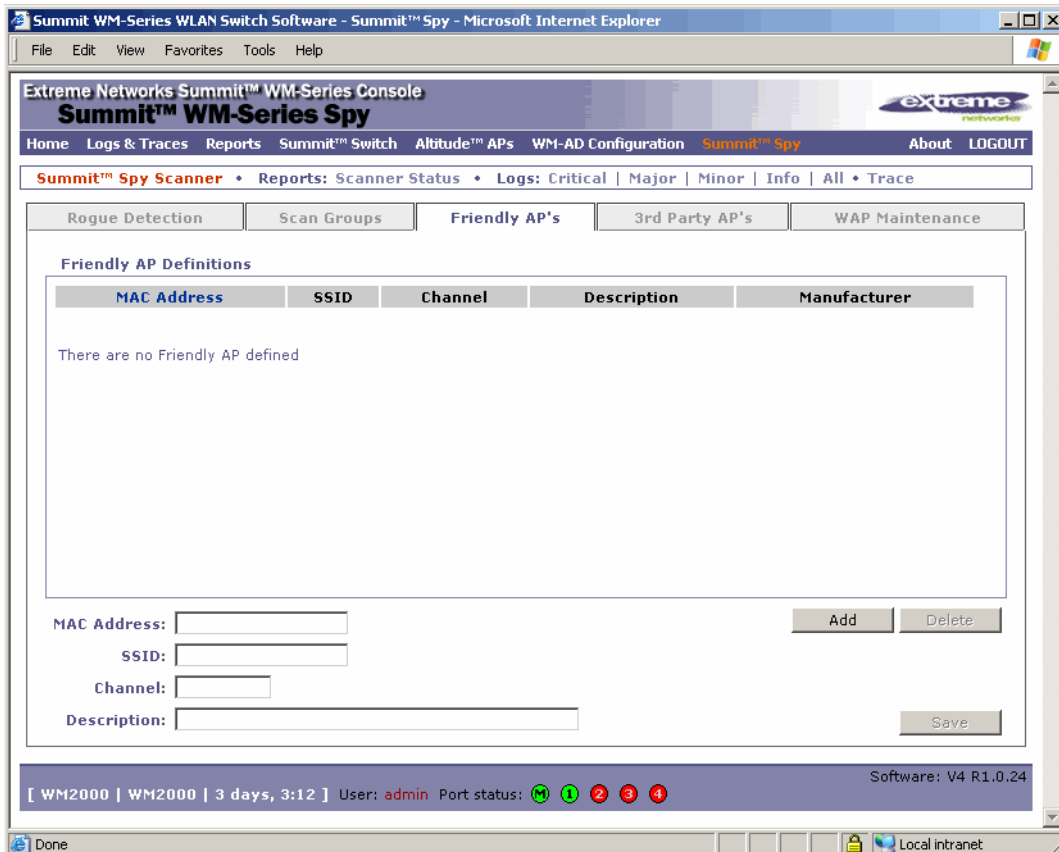
### To delete an AP from the Summit spy scan results:

- From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- Click the **Rogue Detection** tab.
- To delete a specific AP from the Summit spy scan results, click the corresponding **Delete** button. The AP is removed from the list.
- To clear all rogue access points from the Summit spy scan results, click **Clear Detected Rogues**. All APs are removed from the list.

## Working with friendly APs

### To view the friendly APs:

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Friendly AP's** tab.



### To add friendly APs manually:

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Friendly AP's** tab.
- 3 To add friendly access points manually to the **Friendly AP Definitions** list, type the following:
  - **MAC Address** – Specifies the MAC address for the friendly AP
  - **SSID** – Specifies the SSID for the friendly AP
  - **Channel** – Specifies the current operating channel for the friendly AP
  - **Description** – Specifies a brief description for the friendly AP
- 4 Click **Add**. The new access point is displayed in the list above.

**To delete a friendly AP:**

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Friendly AP's** tab.
- 3 To select an access point from the **Friendly AP Definitions** list to delete, click it.
- 4 Click **Delete**. The selected access point is removed from the **Friendly AP Definitions** list.
- 5 To save your changes, click **Save**.

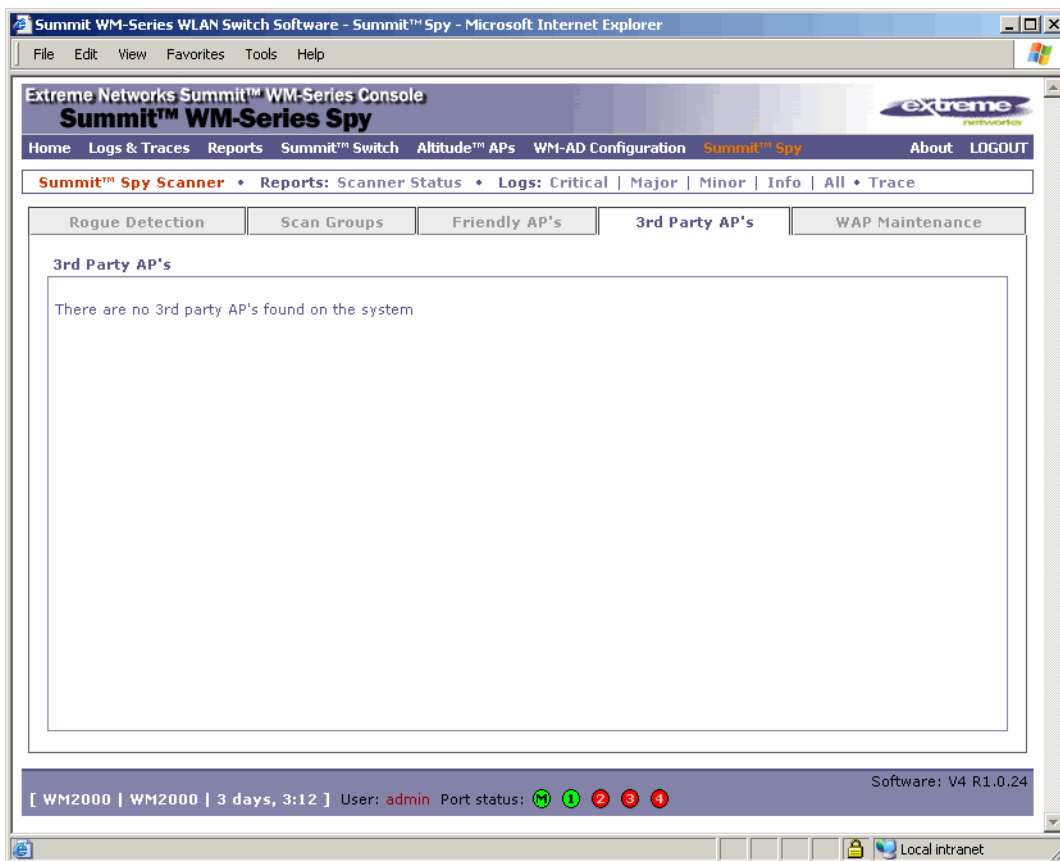
**To modify a friendly AP:**

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Friendly AP's** tab.
- 3 To select an access point from the **Friendly AP Definitions** list to modify, click it.
- 4 Modify the access point by making the appropriate changes.
- 5 To save your changes, click **Save**.

## Viewing the Summit spy list of third-party APs

To view known third-party access points connected to local/remote RF data collectors:

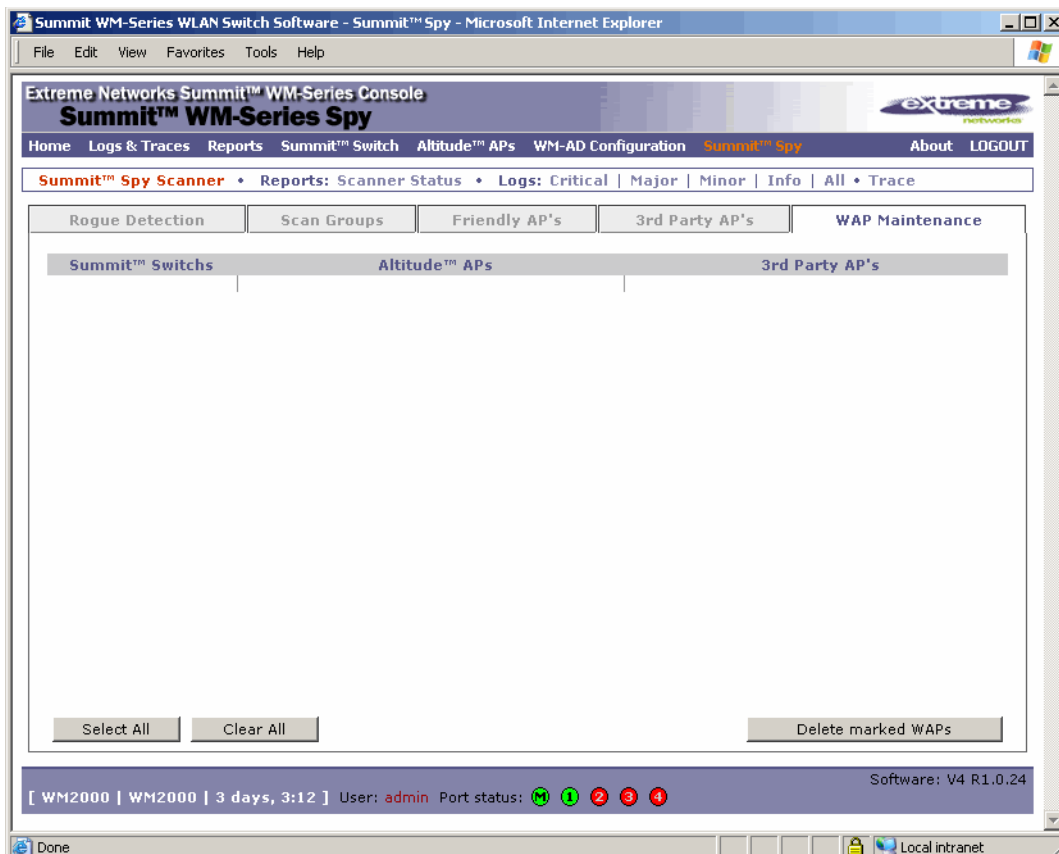
- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **3rd Party AP's** tab.



## Maintaining the Summit spy list of APs

### To maintain the Altitude APs:

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **WAP Maintenance** tab. Inactive APs and known third-party APs are displayed.
- 3 Select the applicable APs.



- 4 To delete the selected APs, click **Delete marked WAPs**.

### NOTE

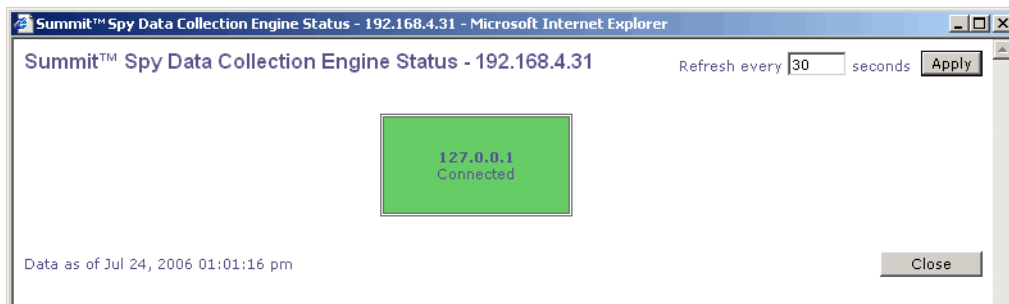
The selected APs are deleted from the Summit spy database, not from the Summit WM series switch database. You can delete the APs from the Summit WM series switch database after you delete them from the Altitude AP Configuration Access Approval screen of the corresponding RF Data Collector Engine. You can also delete the selected third-party APs if they are removed from the corresponding WM-AD in the RF Collector Engine, or if that WM-AD has been deleted from the WM-AD list.

## Viewing the Scanner Status report

When the Summit spy is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

### To view the Summit spy scanner engine status display:

- 1 From the main menu, click **Summit Spy**. The **Summit Spy** screen is displayed.
- 2 Click the **Scanner Status** link. The Scanner Status report is displayed, as shown in the example below.



The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** – The Analysis Engine has connection with the Data Collector on that Summit WM series switch.
- **Yellow** – The Analysis Engine has connected to the communication system of the other controller, but has not synchronized with the Data Collector. Ensure that the Data Collector is running on the remote controller.
- **Red** – The Analysis Engine is aware of the Data Collector and attempting connection.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.



#### NOTE

*If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.*

This chapter describes the various reports and displays available in the Summit WM series switch, access points, and WLAN switch software system.

### Viewing the displays

The following displays are available in the Summit WM series switch, access points, and WLAN switch software system:

- Active Altitude APs
- Active Clients by Altitude AP
- Active Clients by WM-AD
- Port & WM-AD Filter Statistics
- WM-AD Interface Statistics
- Summit Switch Port Statistics
- Altitude AP Availability
- Wired Ethernet Statistics by Altitude AP
- Wireless Statistics by Altitude AP
- Client Location in Mobility Zone
- Mobility Tunnel Matrix

## To view reports and displays:

- 1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.



### NOTE

The two displays on the right-hand side of the screen only appear if the mobility manager function has been enabled for the controller.

- 2 In the **List of Displays**, click the display you want to view (some examples will follow):

Altitude™ AP	Serial	WAP IP	Clients	Home	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	802.11b/g Ch/Tx	802.11a Ch/Tx
0001000401801139	0001000401801139	10.102.1.99	0	Local	0:05:56	228	323	54447	65518	9:05:54	auto/100%	56/100%
<b>Summary</b>	<b>1 active WAP</b>		<b>0</b>									



### NOTE

Statistics are expressed in relation to the AP. Therefore, *Packets Sent* means the AP has sent that data to a client and *Packets Rec'd* means the AP has received packets from a client.

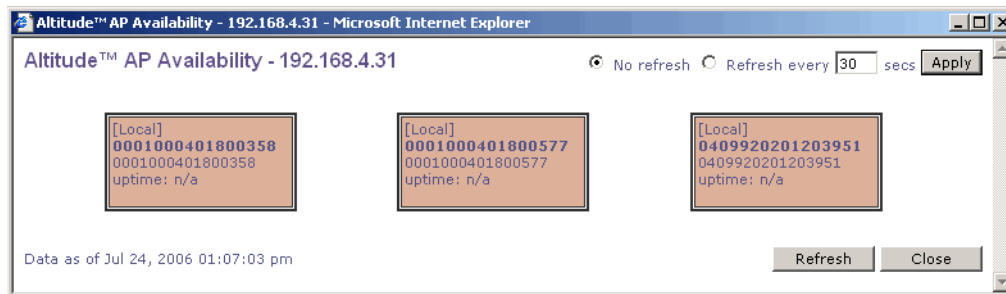


## Viewing the Altitude AP availability display

This display reports the active connection state of an Altitude AP (availability to the Summit WM series switch for service). Depending on the state of the Altitude AP, the following is displayed:

**Green** – Altitude AP is configured on the Summit WM series switch and is presently connected.

**Red** – Altitude AP is configured on the Summit WM series switch but is presently not connected (not available to service this Summit WM series switch).



In normal operations, when the Summit WM series switch **Availability** feature is enabled, the local Altitude APs are green, and the foreign Altitude APs are red. If the other Summit WM series switch fails, and the foreign Altitude APs connect to the current Summit WM series switch, the display will show all Altitude APs as green. If the Altitude APs are not connected they show up as red.

## Viewing statistics for Altitude APs

Two displays are snapshots of activity at that point in time on a selected Altitude AP:

- Wired Ethernet Statistics by Altitude AP
- Wireless Statistics by Altitude AP

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

## To view wired Ethernet statistics by Altitude AP:

- 1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.
- 2 Click the **Wired Ethernet Statistics by Altitude AP** display option. The **Wired Ethernet Statistics by Altitude APs** display opens in a new browser window.

Wired Ethernet Statistics by Altitude™ APs - 192.168.4.31

No refresh Refresh every 30 secs Apply

0001000401800358  
0001000401800577  
0409920201203951

Status Approved IP Address  
MAC Address 00:04:96:0C:AF:00

Statistics	Receive	Transmit
Discarded Packets		
Total Errors		
Unicast Packets		
Multicast Packets		
Broadcast Packets		
Total Packets	0	0
Total Bytes		

Data as of Jul 24, 2006 01:10:16 pm Refresh Export Close

- 3 In the **Wired Ethernet Statistics by Altitude APs** display, click a registered Altitude AP to display its information.

## To view Wireless Statistics by Altitude AP:

- 1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.
- 2 Click the **Wireless Statistics by Altitude AP** display option. The **Wireless Statistics by Altitude APs** display opens in a new browser window.

Wireless Statistics by Altitude™ APs - 192.168.4.31

0001000401800358  
0001000401800577  
0409920201203951

WAP Status: Approved  
WAP IP Address: 802.11b/g 802.11a

MAC Address 00:04:96:0C:AF:08  
SSID lab111  
Operational Rate Set Best data rate  
Channel 1: 2412 MHz  
Power Level Max

Associated Clients There are no active clients on this radio

Statistics	Receive	Transmit
Discarded Packets		
Errors		
Unicast Packets		
Multicast Packets		
Broadcast Packets		
Total Packets	0	0
Total Bytes		

Statistics	802.11 MIB Values
WEP ICV Error Count	
WEP Excluded Count	
Retry Count	
Multiple Retry Count	
RTS Success Count	
RTS Failure Count	
ACK Failure Count	
Frame Duplicate Count	
Transmitted Fragment Count	
Multicast Transmitted Frame Count	
Failed Count	
Received Fragment Count	
Multicast Received Frame Count	
FCS Error Count	
WEP Undecryptable Count	
Transmitted Frame Count	

Data as of Jul 24, 2006 01:11:48 pm

Refresh Export Close

- 3 In the **Wired Statistics by Altitude APs** display, click a registered Altitude AP to display its information.
- 4 Click the appropriate tab to display information for each radio on the Altitude AP.
- 5 To view information on selected associated clients, click **View Client**. The **Associated Clients** display opens in a new browser window.

## To view Active Clients by Altitude AP statistics:

- 1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.
- 2 Click the **Active Clients by Altitude APs** display option. The **Active Clients by Altitude APs** display opens in a new browser window.

Active Clients by Altitude™ AP - 192.168.4.31

Users: 0001000401800577 0001000401800577

0001000401800577 1  
1234567890123456 1

WAP	Client IP	Client MAC	Protocol	BSS MAC	SSID	Auth. Prv.	Filter	Time Conn.	User	Packets Sent	Packets Rec'd	Byte Sen	
<input checked="" type="checkbox"/>	172.29.0.254	00:0F:B5:97:3A:E3	802.11a	00:04:96:0C:B0:D0	tech-test1	None / None	Default	0:17:28	n/a	427	843	3665	
<b>Traffic Summary</b>										1	427	843	3665

Active Users: 2    Search Client by: User name    Search

Data as of Sep 18, 2006 05:44:30 pm    Selected clients:    Add to Blacklist    Disassociate    Refresh    Export

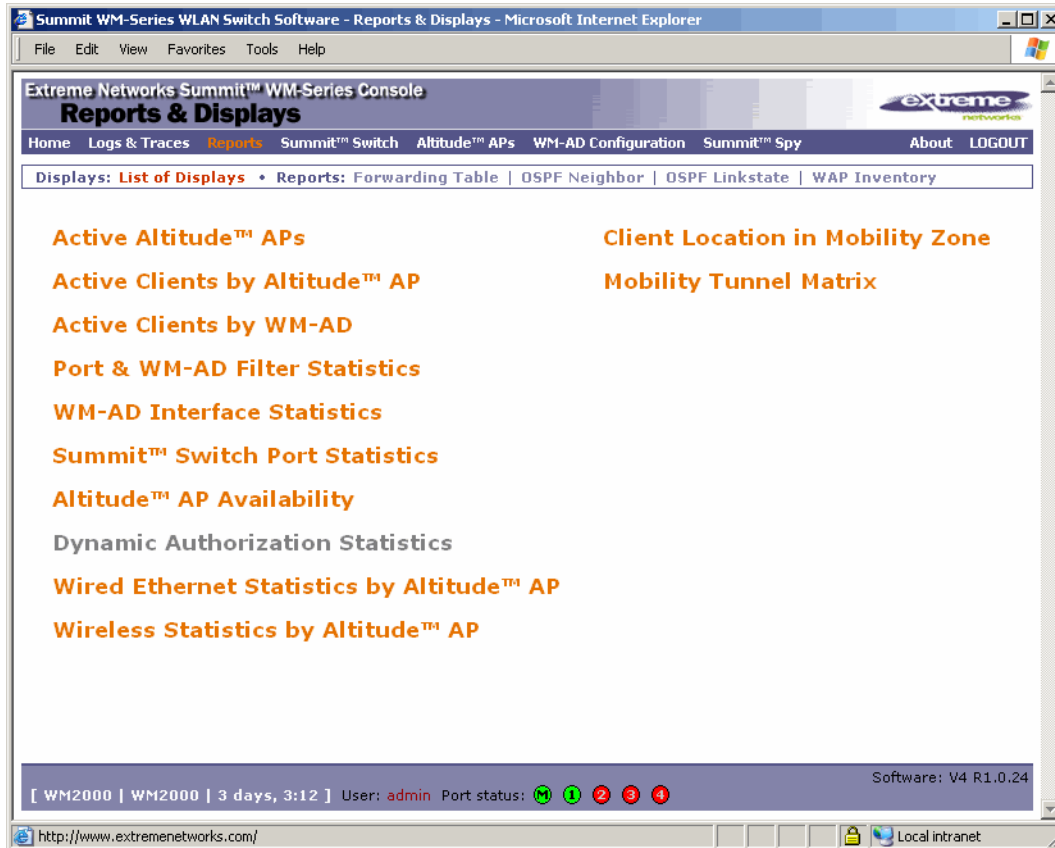
- Statistics are expressed in respect of the AP. Therefore, **Packets Sent** means the AP has sent that data to a client and **Packets Rec'd** means the AP has received packets from a client.
- If the client is authenticated, a green check mark icon is displayed in the first column of the display.
- **Time Conn** is the length of time that a client has been on the system, not just on an AP. If the client roams from one AP to another, the session stays, therefore **Time Conn** does not reset.
- A client is displayed as soon as the client connects (or after refresh of screen). The client disappears as soon as it times out.

## Viewing displays for the mobility manager

When a Summit WM series switch has been configured as a mobility manager, two additional displays appear as options in the **Summit Reports & Displays** screen:

- **Client Location in Mobility Zone** – Displays the active wireless clients and their status

- **Mobility Tunnel Matrix** – Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain



## To view mobility manager displays:

- 1 From the main menu, click **Reports & Displays**. The **Summit Reports & Displays** screen is displayed.
- 2 Click the appropriate mobility manager display:
  - Client Location in Mobility Zone
  - Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** – The mobility manager is in communication with an agent and the data tunnel has been successfully established.
- **Yellow** – The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** – The mobility manager is not in communication with an agent and there is no data tunnel.

## Client Location in Mobility Zone

You can do the following:

- Sort this display by home or foreign controller

- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box
- Define the refresh rates for this display
- Export this information as an xml file

## Mobility Tunnel Matrix

- Provides connectivity matrix of mobility state
- Provides a view of:
  - Tunnel state
    - If a tunnel between controllers is reported down, it is highlighted in red
    - If only a control tunnel is present, it is highlighted in yellow
    - If data and control tunnels are fully established, it is highlighted in green
  - Tunnel Uptime
  - Number of clients roamed (Mobility loading)
  - Local controller loading
  - Mobility membership list

A Summit WM series switch is only removed from the mobility matrix if it is explicitly removed by the administrator from the Mobility permission list. If a particular link between controllers, or the controller is down, the corresponding matrix connections are identified in red color to identify the link.

The Active Clients by WM-AD report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by WM-AD report does not show users that have roamed from other controllers, since the users remain associated with the home controller's WM-AD.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP



### NOTE

*The statistics from the mobility manager are updated every thirty seconds, regardless of the refresh period for the displays.*

## Viewing reports

The following reports are available in the Summit WM series switch, access points, and WLAN switch software system:

- Forwarding Table (routes defined in the Summit WM series switch Routing Protocols screen)
- OSPF Neighbor (if OSPF is enabled in the Routing Protocols screen)
- OSPF Linkstate (if OSPF is enabled in the Routing Protocols screen)
- AP Inventory (a consolidated summary of Altitude AP setup)

## To view reports:

- 1 From the main menu, click **Reports & Displays**. The **Reports & Displays** screen is displayed.
- 2 In the **Reports** list, click the report you want to view:
  - Forwarding Table
  - OSPF Neighbor
  - OSPF Linkstate
  - AP Inventory



### NOTE

The AP Inventory report opens in a new browser window. All other reports appear in the current browser window.

The following is an example of a **Forwarding Table** report:

The screenshot shows a web browser window displaying the 'Summit WM-Series Console Reports & Displays' page. The 'Forwarding Table' report is selected and displayed as a table with the following data:

Route #	Destination	Netmask	Gateway	Interface	Type	Status
1	0.0.0.0	0.0.0.0	10.111.0.2	esa0	OSPF	Active
2	1.1.1.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
3	10.0.1.0	255.255.255.0	10.111.0.2	esa1	Connected	Active
4	10.1.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
5	10.2.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
6	10.3.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
7	10.4.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
8	10.5.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
9	10.6.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
10	10.7.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
11	10.8.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
12	10.11.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
13	10.13.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
14	10.14.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
15	10.15.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
16	10.21.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
17	10.22.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
18	10.23.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
19	10.24.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active
20	10.25.0.0	255.255.255.0	10.111.0.2	esa0	OSPF	Active

At the bottom of the table, there are 'Export' and 'Refresh' buttons. The status bar at the bottom of the console shows: [ WM2000 | WM2000 | 3 days, 3:12 ] User: admin Port status: (4 colored status icons) Software: V4 R1.0.24



### NOTE

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually timeout.

## The following is an example of the AP Inventory report:

Altitude™ AP (Serial)	Port					HW					SW	Country	TA	BD	DV	P/To	P/I	Wired MAC		Description				
	Rdo	Ra	Rb	Rg	DP	BP	SRL	LRL	RT	FT	Ch	PL	BR	ORS	MnBR	MxBR	MxOR	RxDV	TxDV	Pmb	PM	PR	PT	BSS: MAC
0001000401800577 (0001000401800577)	Static Cfg					Local Bridging					Failure Maintn.	Assn	Static Cfg IP			Netmask		Gateway		SWM Search List				
	esa0 (10.208.0.11)					Extreme Altitude 300-2 Detachable Antenna					V4 R0.0.40	United States	enabled	disabled	-	10	2	00:04:96:0C:B0:D0		0001000401800577				
	b/g	-	on	on	1	100	7	4	2346	2346	auto	Max	-	-	1 Mbps	11 Mbps	54 Mbps	Best	Best	Long	Auto	11 Mbps	RTS CTS	00:04:96:0C:B0:D8
	a	on	-	-	1	100	7	4	2346	2346	auto	Max	-	-	6 Mbps	24 Mbps	54 Mbps	Best	Best	-	-	-	-	00:04:96:0C:B0:D0
disabled					-					enabled	DHCP	-			-		-		-					

The following is a description of the column names and abbreviations found in the **AP Inventory** report:

- **Rdo** – Radio
- **Ra** – 802.11a radio. The data entry for an Altitude AP indicates whether the **a** radio is on or off.
- **Rb** – 802.11b protocol enabled. Possible values are **on** or **off**.
- **Rg** – 802.11g protocol enabled. Possible values are **on** or **off**.
- **DP** – DTIM period
- **BP** – Beacon Period
- **SRL** – Short Retry Limit
- **LRL** – Long Retry Limit
- **RT** – RTS Threshold
- **FT** – Fragmentation Threshold
- **Ch** – Channel served by the corresponding radio.
- **PL** – Power Level (Defined in the Altitude AP radio properties pages.)
- **BR** – Basic Rate (Only applies to Altitude APs running 3.1 or earlier.)
- **ORS** – Operational Rate Set (Only applies to Altitude APs running 3.1 or earlier.)
- **MnBR** – Minimum Basic Rate (For more information, see the Altitude AP radio configuration tabs.)
- **MxBR** – Maximum Basic Rate
- **MxOR** – Maximum Operational Rate
- **RxDV** – Receive Diversity
- **TxDV** – Tx Diversity
- **Pmb** – Preamble (long, short)
- **PM** – Protection Mode
- **PR** – Protection Rate
- **PT** – Protection Type
- **BSS** – Basic Service Set
- **MAC** – MAC address
- **BSS: MAC** – Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the Altitude AP serves a BSS/WM-AD. There could be 8 per radio.



- **Port** – Ethernet Port and associated IP address of the interface on the Summit WM series switch through which the Altitude AP communicates.
- **HW** – Hardware version of the Altitude AP.
- **SW** – Software version executing on the Altitude AP.
- **TA** – Telnet access (enabled or disabled).
- **BD** – Broadcast disassociation (enabled or disabled). If enabled, whenever the Altitude AP is going offline in a controlled fashion it will send the disassociation frame to all its clients as a broadcast.
- **DV** – Diversity
- **P/To** – Poll timeout. If polling is enabled, a numeric value.
- **P/I** – Poll interval. If polling is enabled, a numeric value.
- **Wired MAC** – The physical address of the Altitude AP's wired Ethernet interface.
- **Description** – As defined on the **AP Properties** screen.
- **Failure Maintn.** – Maintain MU sessions on Altitude AP when the Altitude AP loses the connection to the Summit WM series switch.
- **Assn** – Assignment (address assignment method)
- **Static Cfg** – Altitude AP's IP address if statically configured (same as the **Static Values** radio button on the **AP Static Configuration** screen).
- **Static Cfg IP** – Statically Configured IP. If the Altitude AP's IP address is configured statically, the IP address is displayed.
- **Netmask** – If the Altitude AP's IP address is configured statically, the netmask that is statically configured for the Altitude AP.
- **Gateway** – If the Altitude AP's IP address is configured statically, the IP address of the gateway router that the Altitude AP will use.
- **HWC Search List** – The list of IP addresses that the Altitude AP is configured to try to connect to in the event that the current connection to the Summit WM series switch is lost.

## To export and save a report in XML:

- 1 On the report screen, click **Export**. A Windows **File Download** dialog is displayed.
- 2 Click the **Save** button. A Windows **Save As** dialog is displayed.



### NOTE

*If your default XML viewer is Internet Explorer or Netscape, clicking Open will open the exported data to your display screen. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.*

- 3 Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.
- 4 Click **Save**. The XML data file is saved in the specified location.



## 10 Performing system maintenance

This chapter describes system maintenance processes, including:

- [Performing Altitude AP client management](#)
- [Resetting the AP to its factory default settings](#)
- [Performing system maintenance tasks](#)
- [Performing Summit WM series switch software maintenance](#)
- [Configuring Summit WM series switch, access points, and WLAN switch software logs and traces](#)

### Performing Altitude AP client management

There are times when for service reasons or security issues, you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected Altitude AP. You can do the following:

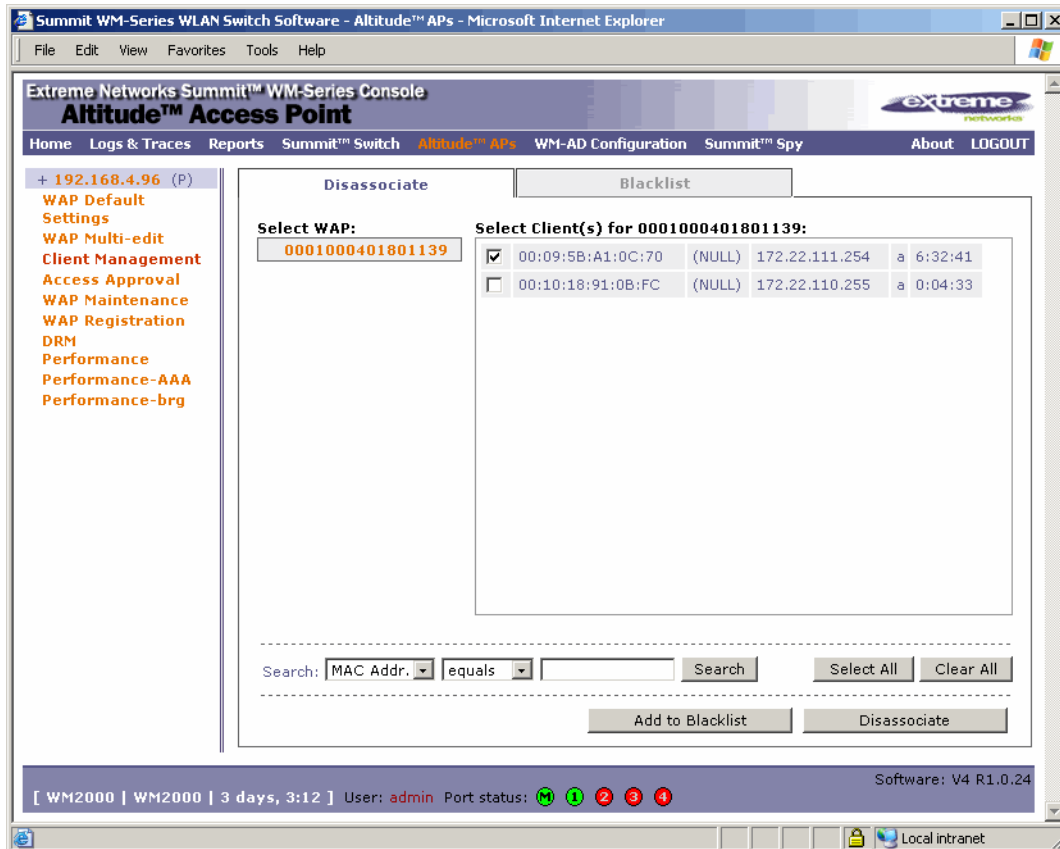
- Disassociate a selected wireless device from its Altitude AP.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the Altitude AP.
- Backup and restore the Summit WM series switch database. For more information, see [“Performing Summit WM series switch software maintenance” on page 210](#).

### Disassociating a client

In addition to the following procedure below, you can also disassociate wireless users directly from the **Active Clients by WM-AD** screen. For more information, see [Chapter 9, “Working with reports and displays.”](#)

## To disassociate a wireless device client:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- 2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



- 3 In the **Select AP** list, click the AP you want to disassociate.
- 4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate, if applicable.

### NOTE

You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the Search box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.

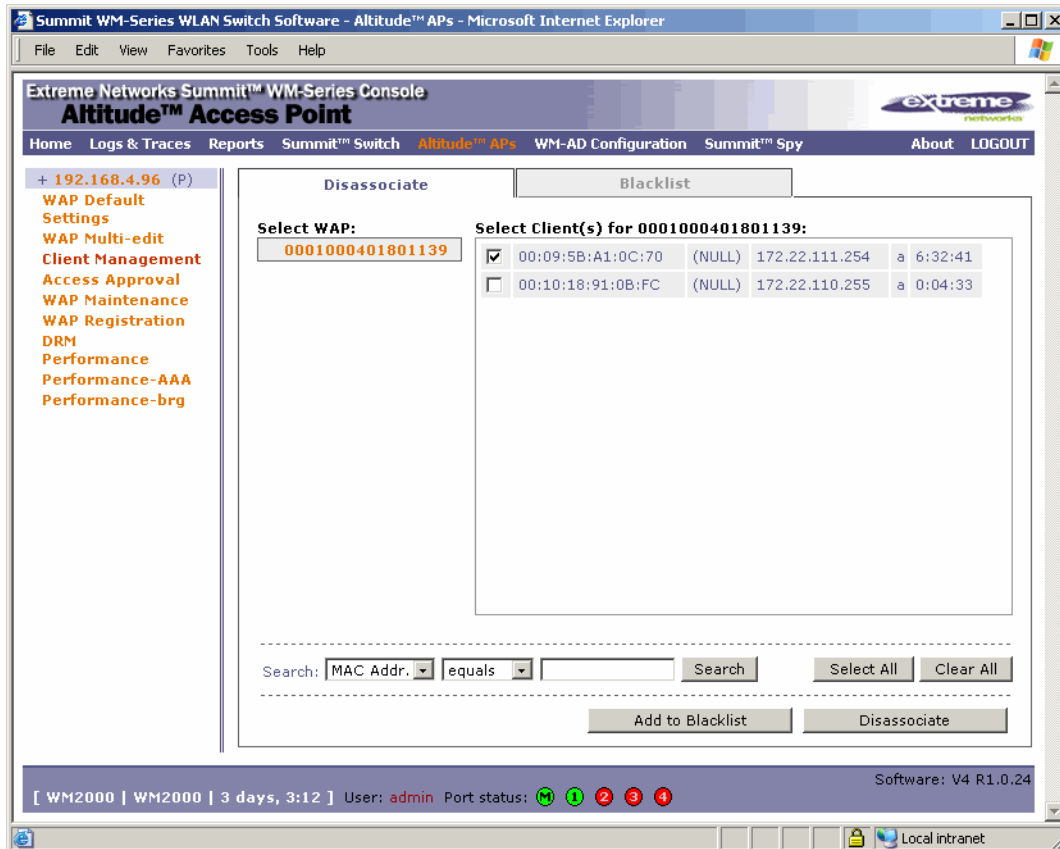
- 5 Click **Disassociate**. The client's session terminates immediately.

## Blacklisting a client

The **Blacklist** tab displays the current list of MAC addresses that are not allowed to associate. A client is added to the blacklist by selecting it from a list of associated APs or by entering its MAC address.

## To blacklist a wireless device client:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- 2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



- 3 In the **Select AP** list, click the AP you want to disassociate.
- 4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate, if applicable.

### NOTE

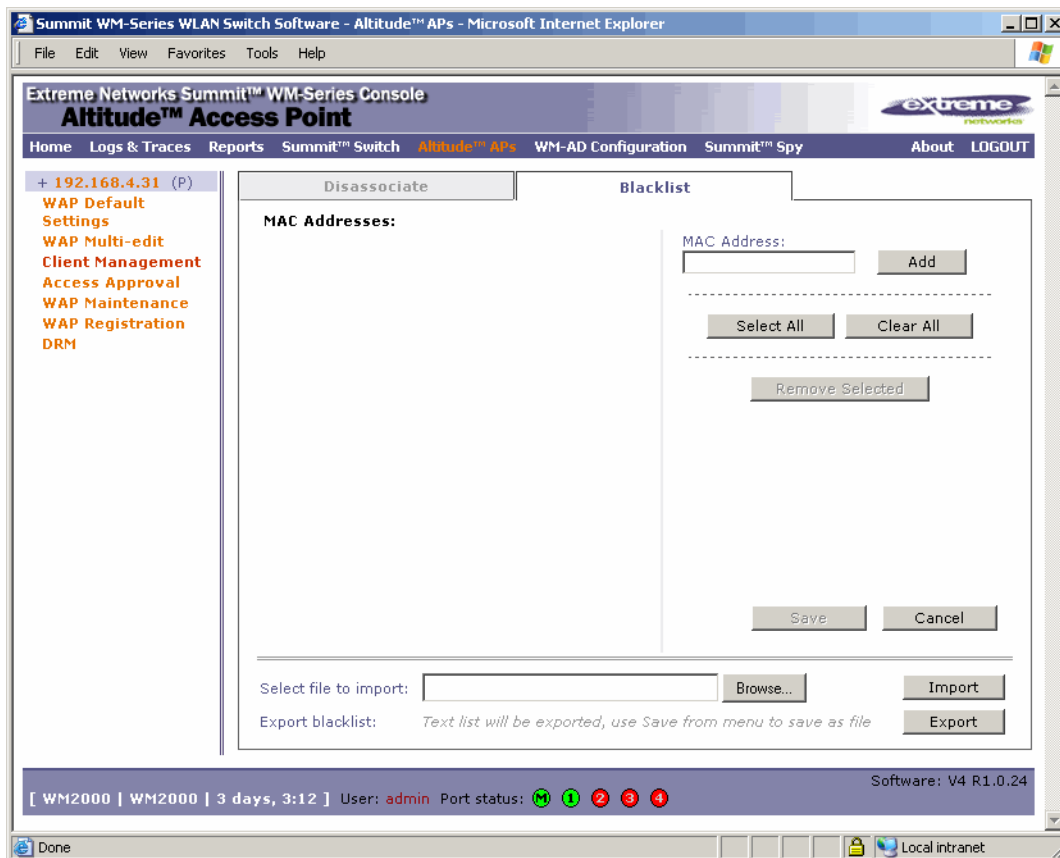
You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the Search box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.

- 5 Click **Add to Blacklist**. The selected wireless client's MAC address is added to the blacklist.

## To blacklist a wireless device client using its MAC address:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- 2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

- Click the **Blacklist** tab.



- To add a new MAC address to the blacklist, in the **MAC Address** box enter the client's MAC address.
- Click **Add**. The client is displayed in the **MAC Addresses** list.

**NOTE**

You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

- To save your changes, click **Save**.

### To clear an address from the blacklist:

- From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- From the left pane, click **Client Management**. The **Disassociate** tab is displayed.
- Click the **Blacklist** tab.
- To clear an address from the blacklist, select the corresponding checkbox in the **MAC Addresses** list.
- Click **Remove Selected**. The selected client is removed from the list.

**NOTE**

You can use the **Select All** or **Clear All** buttons to help you select multiple clients.

- 6 To save your changes, click **Save**.

### To import a list of MAC addresses for the blacklist:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- 2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Blacklist** tab.
- 4 Click **Browse** and navigate to the file of MAC addresses you want to import and add to the blacklist.
- 5 Select the file, and then click **Import**. The list of MAC addresses is imported.

### To export a list of MAC addresses for the blacklist:

- 1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.
- 2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.
- 3 Click the **Blacklist** tab.
- 4 To export the current blacklist, use the browser's save option to save the file as a text (.txt) file. It is recommend that a descriptive file name is used.
- 5 Click **Export**. The saved blacklist file is exported.

## Resetting the AP to its factory default settings

You can reset the Altitude AP to its factory default settings. The AP boot-up sequence includes a random delay interval, followed by a vulnerable time interval. During the vulnerable time interval (2 seconds), the LEDs flash in a particular sequence to indicate that the Summit WM series switch is in the vulnerable time interval. For more information, see [“Understanding the Altitude AP LED status” on page 58](#).

If you power up the AP and interrupt the power during the vulnerable time interval three consecutive times, the next time the AP reboots, it will restore its factory defaults including the user password and the default IP settings.



### WARNING!

---

*The restoration of factory default settings does not erase the non-volatile log.*

### To reset the AP to its factory default settings:

- 1 Reboot the AP.
- 2 Depower and repower the AP during the vulnerable time interval.
- 3 Repeat Step 2 two more times.

When the AP reboots for the fourth time, after having its power supply interrupted three consecutive times, it restores its factory default settings. The AP then reboots again to put the default settings into effect.

## Performing system maintenance tasks

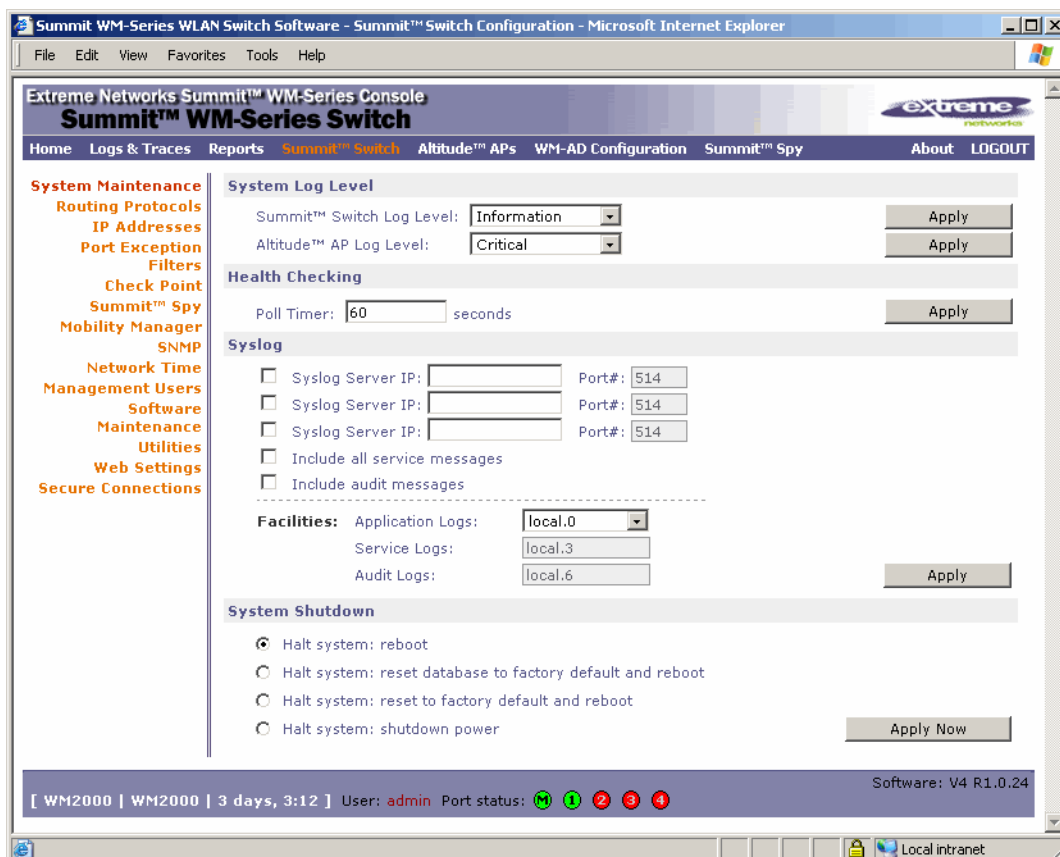
You can perform various maintenance tasks, including:

- Changing the log level
- Setting a poll interval for checking the status of the Altitude APs (Health Checking)
- Enabling and defining parameters for Syslog event reporting
- Forcing an immediate system shutdown, with or without reboot

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

### To change the log levels:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.



- 2 In the **System Log Level** section, from the **Summit Switch Log Level** drop-down list, select the least severe log level for the Controller that you want to receive: **Information**, **Minor**, **Major**, **Critical**. For example, if you select **Minor**, you receive all **Minor**, **Major** and **Critical** messages. If you select **Major** you receive all **Major** and **Critical** messages. The default is **Information**.
- 3 Click **Apply**.



- 4 From the **Altitude AP Log Level** drop-down list, select the least severe log level for the AP that you want to receive: **Information, Minor, Major, Critical**. The default is **Critical**.
- 5 Click **Apply**.

### To set a poll interval:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.
- 3 In the **Health Checking** section, in the **Poll Timer** box, type the time interval (in seconds) for the Summit WM series switch to check that each Altitude AP is connected. The default is **60** seconds.
- 4 Click **Apply**.

### To enable and define parameters for Syslog:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.
- 3 In the **Syslog** section, to enable the **Syslog** function for up to three syslog servers, select the appropriate checkboxes.
- 4 For each enabled syslog server, in the **IP** box, type a valid IP address for the server on the network.
- 5 For each enabled syslog server, in the **Port #** box, type a valid port number to connect on. The default port for syslog is **514**.
- 6 To include all system messages, select the **Include all service messages** checkbox. If the box is not selected, only component messages (logs and traces) are relayed. This setting applies to all three servers. The additional service messages are:
  - DHCP messages reporting users receiving IP addresses
  - Startup Manager Task messages reporting component startup and failure
- 7 To include audit messages, select the **Include audit messages** checkbox.
- 8 From the **Application Logs** drop-down list, select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.
- 9 If the **Include all service messages** checkbox is selected, the **Service Logs** drop-down list becomes selectable. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.
- 10 If you selected the **Include audit messages** checkbox, the **Audit Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.
- 11 To apply your changes, click on the **Apply** button.



#### NOTE

*The syslog daemon must be running on both the Summit WM series switch and on the remote syslog server before the logs can be synchronized. If you change the log level on the Summit WM series switch, you must also modify the appropriate setting in the syslog configuration on remote syslog server.*

Table 17 shows Syslog and Summit WM series switch, access points, and WLAN switch software event log mapping.

**Table 17: Syslog and Summit WM series switch, access points, and WLAN switch software event log mapping**

Syslog Event	Summit WM series switch, access points, and WLAN switch software Event
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information
LOG_DEBUG	Trace

### To force an immediate system shutdown:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **System Maintenance**. The **System Maintenance** screen is displayed.
- 3 To shut down the system, including associated Altitude APs, select the appropriate shut down option:
  - Halt system: reboot
  - Halt system: reset database to factory default and reboot – Restores all aspects of the system configuration to the initial settings. However, the Management IP address and license key are preserved. This permits the user to remain connected through the Management interface.
  - Halt system: reset to factory default and reboot – Resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1 and the license key is removed.
  - Halt system – The system enters the halted state, which stops all functional services and the application. To restart the system, the power to the system must be reset.
- 4 Click **Apply Now**. The system is immediately halted.

## Performing Summit WM series switch software maintenance

You can update the core Summit WM series switch software files, and the Operating System (OS) software using the Software Maintenance function. A facility to backup and restore the Summit WM series switch database is also available. The maintenance interface also includes the product key maintenance, for first-time setup and upgrades, if appropriate. For more information, see [“Applying the product license key” on page 41](#).



### WARNING!

*During a system upgrade from v3.1 to v4 R0.x.x, it is recommended that you install your new v4 license key BEFORE upgrading the software if you have manually configured radio channels.*

If your Summit WM series switch has a v3.1 license key when it is upgraded, the key will be rejected and the Summit WM series switch will revert to a factory default DEMO region setting. Whenever the licensed region changes on the Summit WM series switch, all Altitude APs are changed to **Auto Channel Select** to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost.

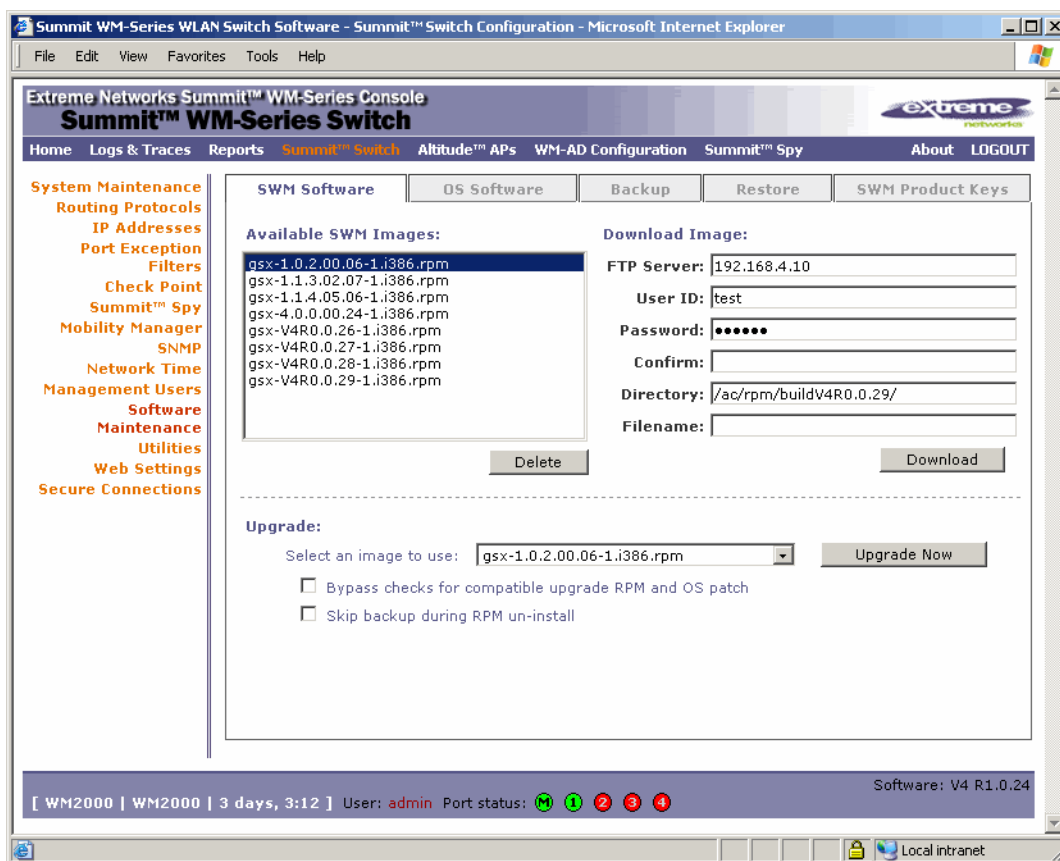
Installing the new license key before upgrading will prevent the Summit WM series switch from changing the licensed region, and in addition, manually configured channel settings will be maintained.

## Updating Summit WM series switch software

You can update the core Summit WM series switch software files using the Software Maintenance function.

### To upgrade Summit WM series switch software:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.



The **Available SWM Images** section displays the list of software versions that have been downloaded and are available.

- 3 In the **Upgrade** section, select an image from the **Select an image to use** drop-down list.

**NOTE**

*It is recommended that the Bypass checks for compatible upgrade RPM and OS patch and the Skip backup during RPM un-install options remain disabled.*

- 4 To launch the upgrade with the selected image, click on the **Upgrade Now** button.
- 5 In the dialog box that is displayed, confirm the upgrade.  
At this point, all sessions are closed. The previous software is uninstalled automatically. The new software is installed. The Summit WM series switch reboots automatically. The database is updated and migrated.

### To download a new Summit WM series switch software image:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 To download a new image to be added to the list, in the **Download Image** section type the following:
  - **FTP Server** – The IP of the FTP server to retrieve the image file from.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
  - **Filename** – The name of the image file to retrieve.
  - **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
- 4 Click **Download**. The image is downloaded and added to the list.

### To delete a Summit WM series switch software image:

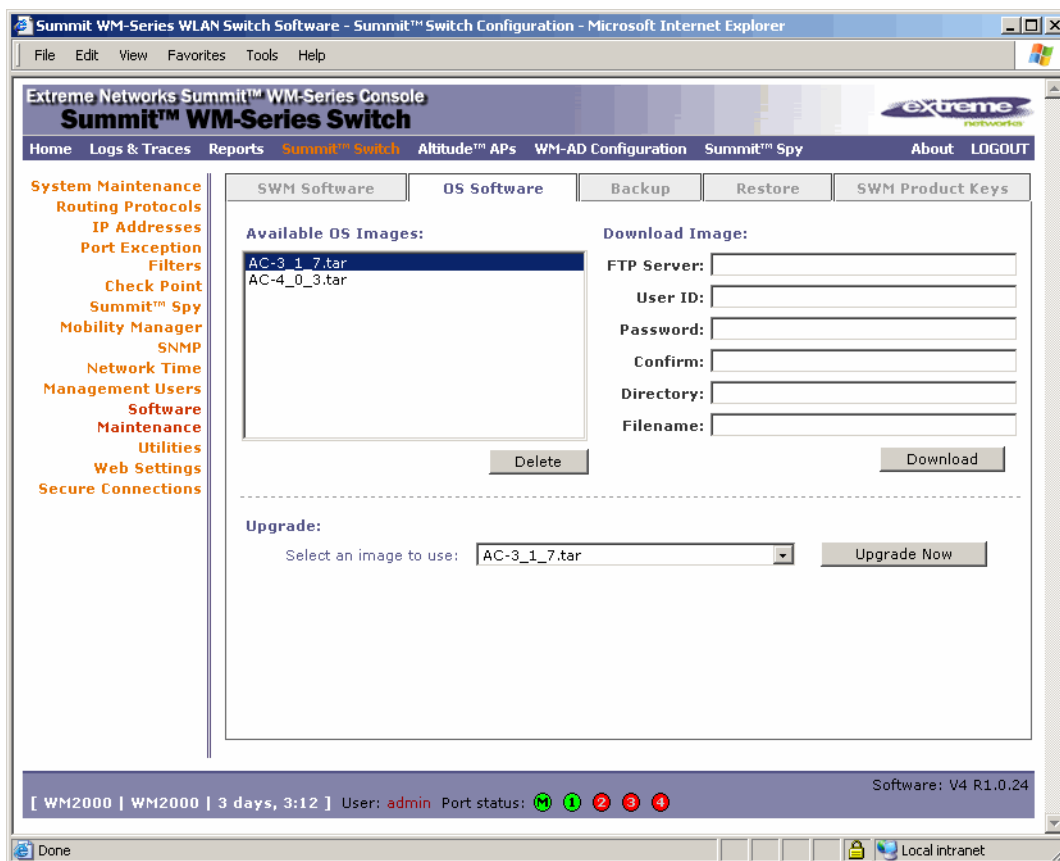
- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 To delete a software image from the list, in the **Available SWM Images** list, click the image.
- 4 Click **Delete**. The image is removed from the list.

## Updating operating system software

You can update the Operating System (OS) software using the Software Maintenance function.

## To upgrade operating system software:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **OS Software** tab.



The **Available OS Images** section displays the list of software versions that have been downloaded and are available.

- 4 In the **Upgrade** section, select an image from the **Select an image to use** drop-down list.
- 5 To launch the upgrade with the selected image, click **Upgrade Now**.
- 6 In the dialog box that is displayed, confirm the upgrade.

At this point, all sessions are closed. The previous software is uninstalled automatically. The new software is installed. The Summit WM series switch reboots automatically.

## To download a new operating system software image:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **OS Software** tab.

- 4 To download a new image to be added to the list, in the **Download Image** section type the following:
  - **FTP Server** – The IP of the FTP server to retrieve the image file from.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
  - **Filename** – The name of the image file to retrieve.
  - **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
- 5 Click **Download**. The image is downloaded and added to the list.

### To delete a Summit WM series switch software image:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **OS Software** tab.
- 4 To delete a software image from the list, in the **Available OS Images** list, click the image.
- 5 Click **Delete**. The image is removed from the list.

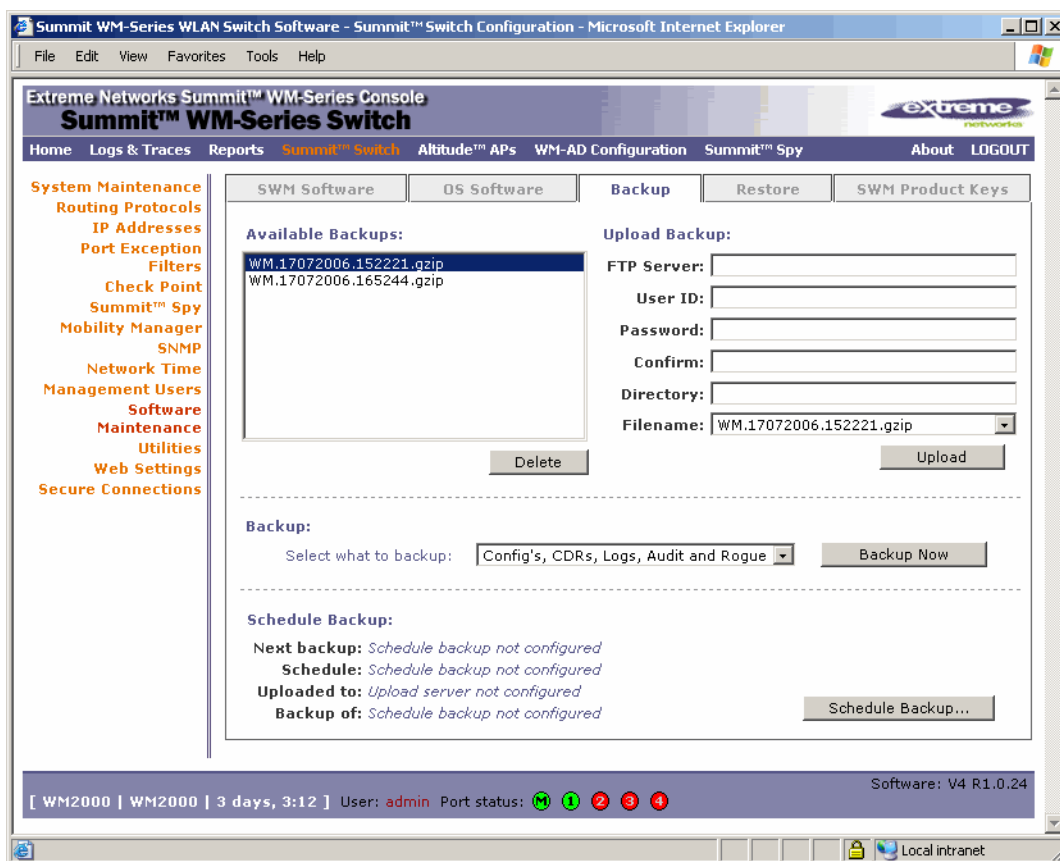
## Backing up Summit WM series switch software

You can backup the Summit WM series switch database. You can also schedule the backups to occur. When a scheduled backup is defined, you can configure to have the scheduled backup copied to an FTP server when the backup is complete.

### To back up the Summit WM series switch software:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

- 3 Click the **Backup** tab.



The **Available Backups** section displays the list items that have been backed up and are available.

- 4 In the **Backup** section, select an item from the **Select what to backup** drop-down list.
- 5 To launch the backup with the selected items, click on the **Backup Now** button.
- 6 In the dialog box that is displayed, confirm the backup. The items are backed up.

### To upload a new backup:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **Backup** tab.
- 4 To upload a new backup, which will be added to the list, in the **Upload Backup** section type the following:
  - **FTP Server** – The IP of the FTP server to retrieve the image file from.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – The directory on the server where the image file will be stored.
  - **Filename** – The name that will be given to the image file when it is stored on the FTP server.

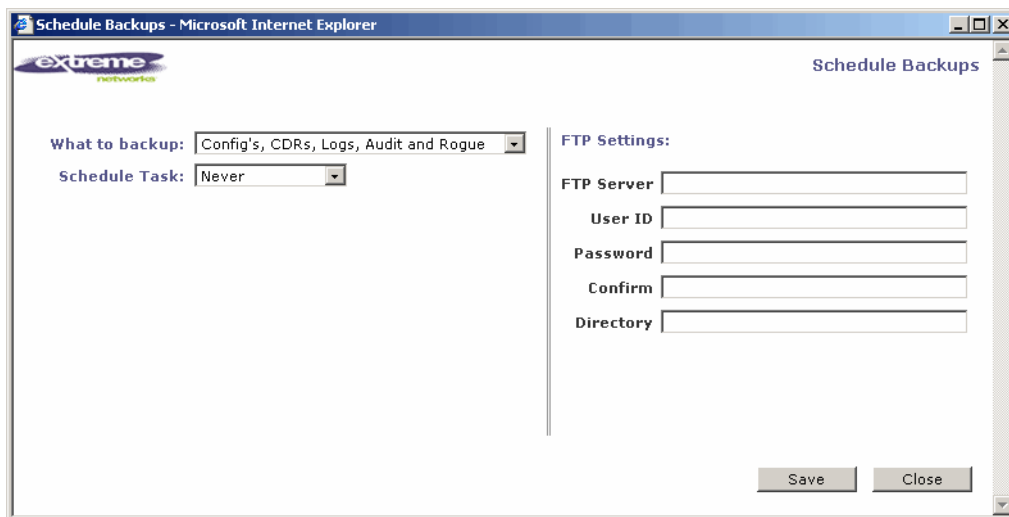
- **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
- 5 Click **Upload**. The backup is uploaded and added to the list.

### To delete a backup:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **Backup** tab.
- 4 To delete a backup from the list, in the **Available Backups** list, click the backup.
- 5 Click **Delete**. The backup is removed from the list.

### To schedule a backup:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
- 3 Click the **Backup** tab.
- 4 Click **Schedule Backup**. The **Schedule Backups** screen is displayed.



- 5 In the **What to backup** drop-down list, select what you want to backup:
  - Config's, CDRs, Logs, Audit and Rogue
  - Configurations only
  - CDRs only
  - Logs only
  - Audit only
  - Rogue only



- 6 In the **Schedule task** drop-down list, select the frequency of the backup:
  - Daily
  - Weekly
  - Monthly
  - Never
- 7 In the **FTP settings** section, type the following:
  - **FTP Server** – The IP of the FTP server to where the scheduled backup will be copied to.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – The directory on the server where the image file will be stored.
- 8 To save your changes, click **Save**.

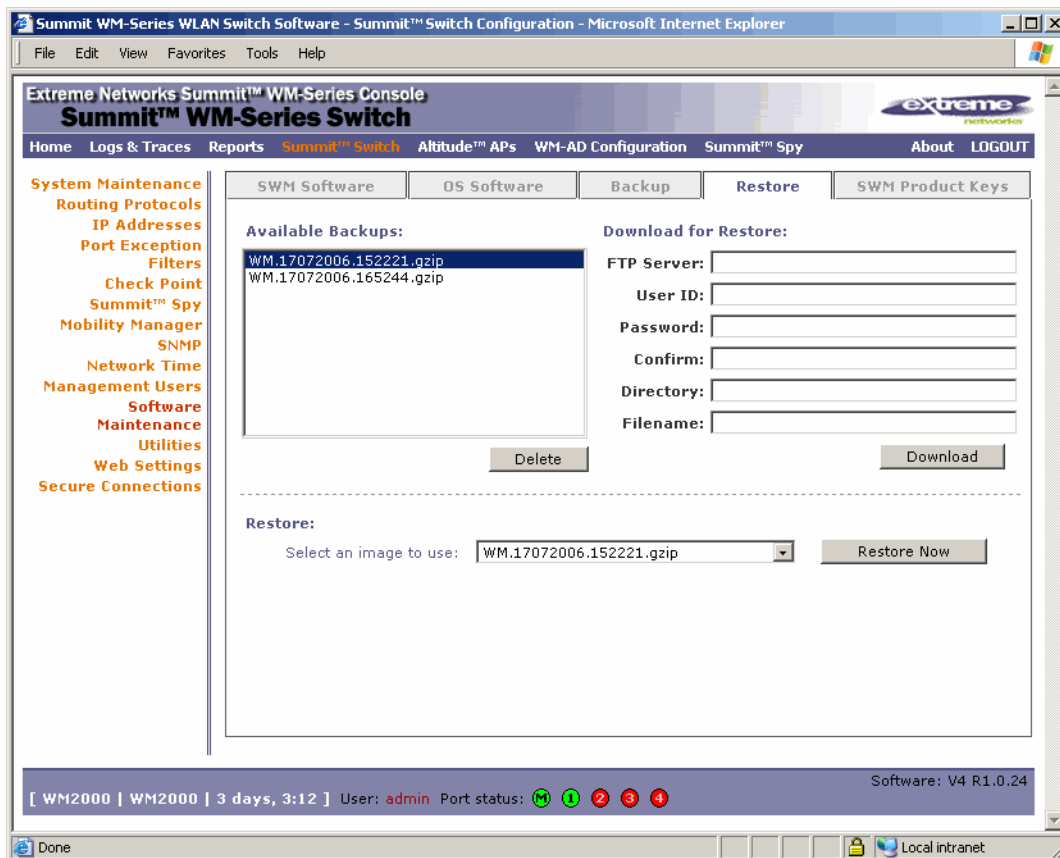
## Restoring Summit WM series switch software

You can restore the Summit WM series switch database.

### To restore the Summit WM series switch software:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

- 3 Click the **Restore** tab.



The **Available Backups** section displays the list items that have been backed up and are available.

- 4 In the **Restore** section, select an item from the **Select an image to use** drop-down list.
- 5 To launch the backup with the selected items, click on the **Restore Now** button.
- 6 In the dialog box that is displayed, confirm the restore. The image is restored.

### To download for restore:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **System Maintenance** screen is displayed.
- 3 Click the **Restore** tab.
- 4 To download an image for restore, which will be added to the list, in the **Download for Restore** section type the following:
  - **FTP Server** – The FTP server to retrieve the image file from.
  - **User ID** – The user ID that the controller should use when it attempts to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
  - **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
  - **Filename** – The name of the image file to retrieve.

- **Platform** – The AP hardware type to which the image applies. There are several types of AP and they require different images.
- 5 Click **Download**. The image is downloaded and added to the list.

### To delete a backup available for restore:

- 1 From the main menu, click **Summit Switch Configuration**. The **Summit Switch Configuration** screen is displayed.
- 2 From the left pane, click **Software Maintenance**. The **System Maintenance** screen is displayed.
- 3 Click the **Restore** tab.
- 4 To delete a backup from the list, in the **Available Backups** list, click the backup.
- 5 Click **Delete**. The backup is removed from the list.

## Upgrading a Summit WM series switch using SFTP

You can upload an image file to the Summit WM series switch using Secure FTP (SFTP). The Summit WM series switch supports any SFTP client.



### NOTE

You must enable management traffic before you try to connect with a SFTP client. Specify the exact image path for the corresponding SW package (see directory information below). Otherwise, the Summit WM series switch cannot locate them for SW upgrades/updates.

### To upload an image file:

- 1 Launch the SFTP client, point it to the Summit WM series switch and login in. The exact details of how to do this will depend on the client used. The following uses putty as an example:

```

C:\> Command Prompt - ssh -l admin 192.168.3.63
[admin@LAB63-G-117test controller]# ls /var/controller/osupgrade
AC-0_0_1.tar AC-4_0_2.tar
[admin@LAB63-G-117test controller]# cd /var/controller/upgrade
[admin@LAB63-G-117test upgrade]# ls
AC-RH-4_0_5.tar gss-U4R0.0.40-1.i386.rpm gss-U4R0.95.131-1.i386.rpm updateos
[admin@LAB63-G-117test upgrade]# cd /var/controller/osupgrade
[admin@LAB63-G-117test osupgrade]# ls
AC-0_0_1.tar AC-4_0_2.tar
[admin@LAB63-G-117test osupgrade]# _

```

- 2 Change to the directory to receive the uploaded file:
  - For AP images change to: /var/tftp/chantry
  - For Summit WM series switch images change to: /var/controller/upgrade
  - For OS archives change to: /var/controller/osupgrade
- 3 Upload the image file using the SFTP client upload feature.
- 4 To complete a Summit WM series switch upgrade or an AP upgrade go to the appropriate **Software Maintenance** screen. For more information, see [“Updating Summit WM series switch software”](#) on page 211 or [“Updating operating system software”](#) on page 212.

## Configuring Summit WM series switch, access points, and WLAN switch software logs and traces

The system stores configuration data and log files. These files include:

- event and alarm logs (triggered by events)
- trace logs (triggered by component activity)
- accounting files (created every 30 minutes, to a maximum of six files)

The files are stored in the operating system and have a maximum size of one GB. The accounting files are stored in flat files in a directory that is created every day. Eight directories are maintained in a circular buffer (when all are full, the most recent replaces the earliest).

## Viewing log, alarm and trace messages

The Summit WM series switch generates three types of messages:

- Logs (including alarms) – Messages that are triggered by events
- Audits – Files that record administrative changes made to the system (the GUI Audit displays changes to the Graphical User Interface on the Summit WM series switch)
- Traces – Messages that display activity by component, for system debugging, troubleshooting and internal monitoring of software



### NOTE

*In order for the Debug Info option on the Altitude AP Traces screen to return Trace messages, this option must be enabled while Altitude AP debug commands are running. To do so, you need to run an Altitude AP CLI command to turn on a specific Altitude AP debug. Once the CLI command is run, select the Debug Info option, and then click Retrieve Traces. For more information, see the Summit WM series switch, access points, and WLAN switch software CLI Reference Guide.*

*Because Altitude AP debugging can affect the normal operation of Altitude AP service, enabling debugging is not recommended, unless specific instructions are provided.*

## Logs including alarms

The log messages contain the time of event, severity, source component and any details generated by the source component. The messages are classified at four levels of severity:

- Informational, the activity of normal operation
- Minor (alarm)
- Major (alarm)
- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with.

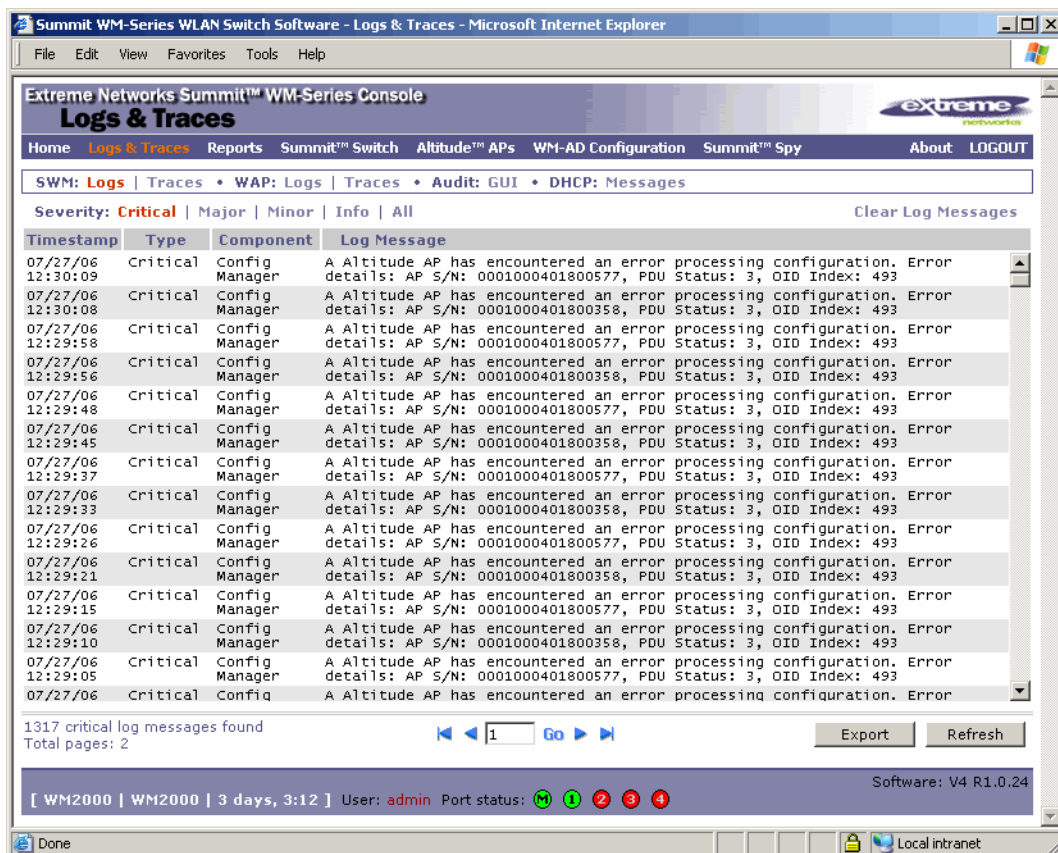
Examples of events on the Summit WM series switch that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the Summit WM series switch
- Software upgrade failure on the Altitude AP
- Detection of rogue access point activity without valid ID

If SNMP is enabled on the Summit WM series switch, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.

## To view logs:

- 1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.
- 2 Click one of the **Log** tabs. The following is an example of the Summit WM series switch logs:



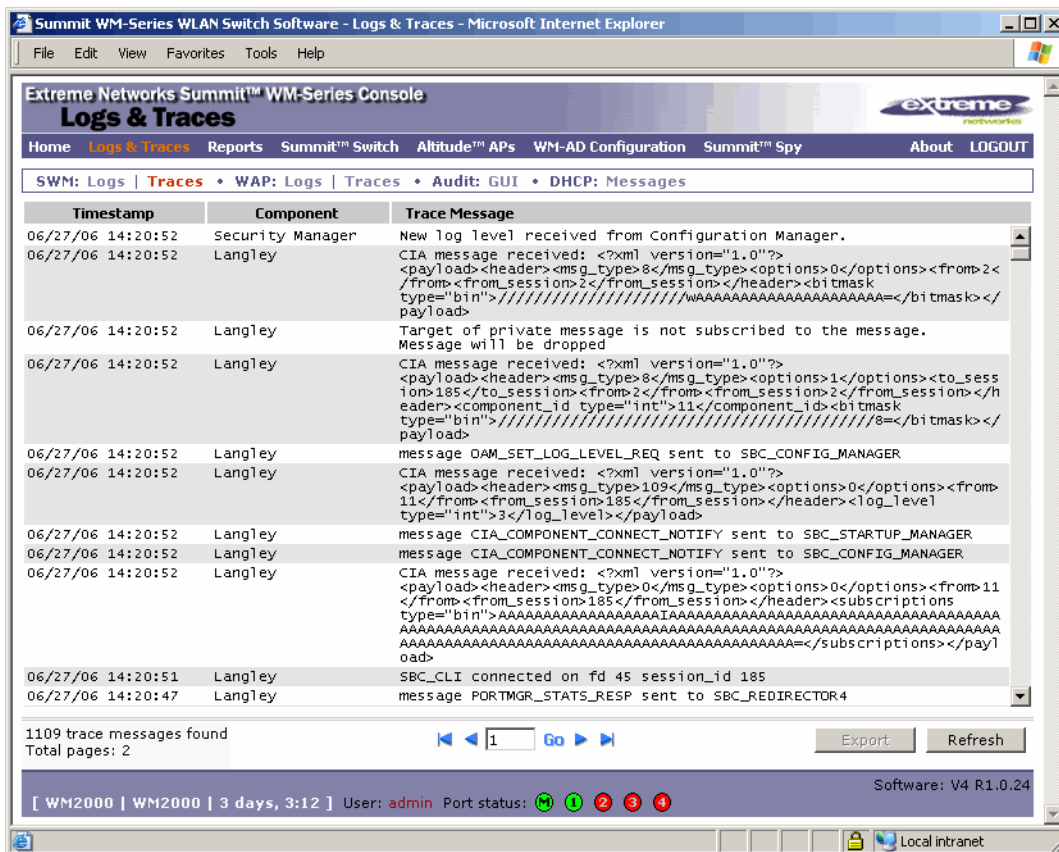
The events are displayed in chronological order, sorted by the **Timestamp** column.

- 3 To sort the display by **Type** or **Component**, click the appropriate column heading.
- 4 To filter the logs by severity, in order to display only **Info**, **Minor**, **Major**, or **Critical** logs, click the appropriate **Log** tab at the top of the screen.
- 5 To refresh the information in any display, click **Refresh**.
- 6 To export information from a display as an HTML file, click the **Export** button.

The component called “Langley” is the term for the inter-process messaging infrastructure on the Summit WM series switch.

**To view traces:**

- 1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.
- 2 Click one of the **Traces** tabs. The following is an example of the Summit WM series switch traces:



The events are displayed in chronological order, sorted by the **Timestamp** column.

- 3 To sort the display by **Type** or **Component**, click the appropriate column heading.
- 4 To filter the traces by severity, in order to display only **Info**, **Minor**, **Major**, or **Critical** traces, click the appropriate **Traces** tab at the top of the screen.
- 5 To refresh the information in any display, click **Refresh**.
- 6 To export information from a display as an HTML file, click the **Export** button.

## To view audits:

- 1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.
- 2 Click the **Audit: GUI** tab. The **Audit** screen is displayed.

The screenshot shows the Summit WM-Series Console interface. The main content area displays a table of audit messages. The table has the following columns: Timestamp, User, Section, Page, and Audit Message. The messages are sorted by timestamp in chronological order.

Timestamp	User	Section	Page	Audit Message
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Mobility SLP Registration enabled
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Heartbeat changed from [WM] to [5]
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Port changed from [10.0.0.1] to [10.111.0.5]
07/24/06 13:04:18	admin	Sys Mgmt	Mobility	Role changed from [None] to [Manager]
07/24/06 12:54:08	admin	Sys Mgmt	SWM-S	Summit( Spy Data Collection Engine enabled
07/24/06 12:54:08	admin	Sys Mgmt	SWM-S	Summit( Spy Analysis Engine enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	esa1 enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	esa0 enabled
07/24/06 12:48:45	admin	Sys Mgmt	IP Addr	Summit( Switch interfaces has been modified.
07/24/06 12:37:56	admin	Sys Mgmt	Users	User guest added to user_read
07/21/06 17:30:54	admin	WM-AD Cfg	Common	WM-AD id 4 has been renamed from [CP_New] to [AAA_New]
07/21/06 17:17:50	admin	WM-AD Cfg	RAD Policy	WM-AD RADIUS policies has been updated for WM-AD lab111
07/21/06 16:33:51	admin	WM-AD Cfg	Common	WM-AD [CP_New] (id: 4) has been created.
07/21/06 14:17:04	admin	WAP5	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 14:16:38	admin	WAP5	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0001000401800358, radio id 1
07/21/06 14:11:43	admin	WAP5	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 14:11:43	admin	WAP5	Prop	Power Level changed from [5] to [1] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAP5	Prop	TX Diversity changed from [3] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAP5	Prop	RX Diversity changed from [3] to [2] for WAP serial 0409920201203951, radio id 7
07/21/06 13:56:25	admin	WAP5	Prop	Short Preamble Invoked changed from [] to [2] for WAP serial 0409920201203951, radio id 7

Below the table, there are 113 audit messages found. Total pages: 1. Navigation buttons include 'Clear Audits', 'Export', and 'Refresh'. The status bar at the bottom shows 'Software: V4 R1.0.24' and 'User: admin Port status: (M) (G) (R) (B) (Y) (O)'.

The events are displayed in chronological order, sorted by the **Timestamp** column.

- 3 To sort the display by **User**, **Section**, **Page**, or **Audit Message**, click the appropriate column heading.
- 4 To clear the audits from the list, click **Clear Audits**.
- 5 To refresh the information in any display, click **Refresh**.
- 6 To export information from a display as an HTML file, click the **Export** button.



## To clear logs:

- 1 From the main menu, click **Logs & Traces**. The **Logs & Traces** screen is displayed.
- 2 Click one of the **Log** tabs. The following is an example of the Summit WM series switch logs:

The screenshot shows the 'Logs & Traces' interface in a Microsoft Internet Explorer browser window. The page title is 'Summit WM-Series WLAN Switch Software - Logs & Traces - Microsoft Internet Explorer'. The main content area is titled 'Extreme Networks Summit™ WM-Series Console' and 'Logs & Traces'. There are navigation tabs for 'Home', 'Logs & Traces', 'Reports', 'Summit™ Switch', 'Altitude™ APs', 'WM-AD Configuration', 'Summit™ Spy', 'About', and 'LOGOUT'. Below the tabs, there are sub-tabs for 'SWM: Logs', 'Traces', 'WAP: Logs', 'Traces', 'Audit: GUI', and 'DHCP: Messages'. A 'Severity' filter is set to 'Critical', with options for 'Major', 'Minor', and 'Info'. A 'Clear Log Messages' button is visible. The main log table has the following columns: 'Timestamp', 'Type', 'Component', and 'Log Message'. The log messages are as follows:

Timestamp	Type	Component	Log Message
07/27/06 12:30:09	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:30:08	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:58	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:56	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:48	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:45	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:37	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:33	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:26	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:21	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:15	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06 12:29:10	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800358, PDU Status: 3, OID Index: 493
07/27/06 12:29:05	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error details: AP S/N: 0001000401800577, PDU Status: 3, OID Index: 493
07/27/06	Critical	Config Manager	A Altitude AP has encountered an error processing configuration. Error

At the bottom of the log table, it says '1317 critical log messages found' and 'Total pages: 2'. There are navigation buttons for 'Go' and 'Export', and a 'Refresh' button. The status bar at the bottom shows 'Software: V4 R1.0.24' and 'User: admin'.

The events are displayed in chronological order, sorted by the **Timestamp** column.

- 3 To clear the logs, click **Clear Log Messages**.



## Networking terms and abbreviations

### A

- AAA** Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.
- Access Point (AP)** A wireless LAN transceiver or “base station” that can connect a wired LAN to one or many wireless devices.
- Ad-hoc mode** An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)
- AES** Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits. AES was created by the National Institute of Standards and Technology (NIST). AES is a privacy transform for IPSec and Internet Key Exchange (IKE). AES has a variable key length - the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.
- AES-CCMP** AES uses the Counter-Mode/CBC-MAC Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.
- ARP** Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.
- Association** A connection between a wireless device and an Access Point.
- asynchronous** Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

**B**

**BSS** Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also IBSS.

**C**

**Captive Portal** A browser-based authentication mechanism that forces unauthenticated users to a Web page. Sometimes called a “reverse firewall”.

**CDR** Call Data (Detail) Record  
In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call.

In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database

**CHAP** Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

**CLI** Command Line Interface.

**Collision** Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.

**D**

**Datagram** A datagram is “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” (RFC1594). The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.

**Decapsulation** See tunnelling.

## D (Continued)

<b>Device Server</b>	A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.
<b>DHCP</b>	<p>Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.</p> <p>DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (IETF RFC1531.)</p> <p>Option 78 specifies the location of one or more SLP Directory Agents. Option 79 specifies the list of scopes that a SLP Agent is configured to use.(RFC2610 - DHCP Options for Service Location Protocol)</p>
<b>Directory Agent (DA)</b>	<p>A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.</p> <p>With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.</p> <p>For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.</p> <p>(SLP version 2, RFC2608, updating RFC2165)</p>
<b>Diversity antenna and receiver</b>	<p>The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal.</p> <p>Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.</p>
<b>DNS</b>	Domain Name Server
<b>DSSS</b>	<p>Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)</p>

## D (Continued)

<b>DTIM</b>	DTIM delivery traffic indication message (in 802.11 standard)
<b>Dynamic WEP</b>	The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1X standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1X standard supplemented the EAP protocol with a mechanism to send an encryption key to an Altitude AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.

## E

<b>EAP-TLS</b> <b>EAP-TTLS</b>	<p>EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.</p> <p>In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.</p> <p>EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.</p> <p>EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.</p> <p><i>(See also PEAP)</i></p>
<b>ELA (OPSEC)</b>	Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.
<b>Encapsulation</b>	<i>See</i> tunnelling.
<b>ESS</b>	Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. <i>(See</i> BSS and SSID.)

## F

**FHSS** Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that “hops” in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)

**Fit, thin and fat APs**

A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required.

A fit AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management.

A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.

**FQDN** Fully Qualified Domain Name. A “friendly” designation of a computer, of the general form computer.[subnetwork].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.

**FTM** Forwarding Table Manager

**FTP** File Transfer Protocol

## G

**Gateway** In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

**Gigabit Ethernet** The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.

**GUI** Graphical User Interface

## H

<b>Heartbeat message</b>	<p>A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive. In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.</p>
<b>Host</b>	<p>(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines.</p> <p>(2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.</p>
<b>HTTP</b>	<p>Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)</p>
<b>HTTPS</b>	<p>Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.</p>

## I

<b>IBSS</b>	<p>Independent Basic Service Set. <i>See</i> BSS. An IBSS is the 802.11 term for an adhoc network. <i>See</i> adhoc network.</p>
<b>ICMP</b>	<p>Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.</p>
<b>ICV</b>	<p>ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (<i>See</i> WPA and MIC)</p>
<b>IE</b>	<p>Internet Explorer.</p>
<b>IEEE</b>	<p>Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.</p>
<b>IETF</b>	<p>Internet Engineering Task Force, the main standards organization for the Internet.</p>



## I (Continued)

<b>Infrastructure Mode</b>	An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (See ad-hoc mode and BSS.)
<b>Internet or IP telephony</b>	<p>IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network).</p> <p>An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support Quality of Service (QoS) are being implemented to improve this.</p>
<b>IP</b>	Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
<b>IPC</b>	Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.
<b>IPsec</b> <b>IPsec-ESP</b> <b>IPsec-AH</b>	<p>Internet Protocol security (IPSec)</p> <p>Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram. Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver. IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.</p>

## I (Continued)

**isochronous** Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.

**ISP** Internet Service Provider.

**IV** IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (*See* WPA and TKIP)

## L

**LAN** Local Area Network.

### License installation

**LSA** Link State Advertisements received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies. *See* also OSPF.

## M

**MAC** Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

**MAC address** Media Access Control address. A hardware address that uniquely identifies each node of a network.

**MIB** Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).

## M (Continued)

<b>MIC</b>	<p>Message Integrity Check or Code (MIC), also called “Michael”, is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.</p> <p>Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (<i>See</i> WPA, TKIP and ICV).</p>
<b>MTU</b>	<p>Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.</p>
<b>MU</b>	<p>Mobile Unit, a wireless device such as a PC laptop.</p>
<b>multicast, broadcast, unicast</b>	<p>Multicast: transmitting a single message to a select group of recipients.          Broadcast: sending a message to everyone connected to a network.          Unicast: communication over a network between a single sender and a single receiver.</p>

## N

<b>NAS</b>	<p>Network Access Server, a server responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)</p>
<b>NAT</b>	<p>Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.</p>
<b>Netmask</b>	<p>In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The “.0” in the “255.255.255.0” netmask allows the specific host computer address to be visible.</p>
<b>NIC</b>	<p>Network Interface Card. An expansion board in a computer that connects the computer to a network.</p>
<b>NMS</b>	<p>Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.</p>

## N (Continued)

**NTP** Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)

## O

**OFDM** Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.

**OID** Object Identifier.

**OPSEC** OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the "Secured by Check Point" seal have been tested to guarantee integration and interoperability.

**OS** Operating system.

**OSI** Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.

**OSI Layer 2** At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sublayers:

- the Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking
- The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.

**OSI Layer 3** The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

## O (Continued)

**OSPF** Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place. (RFC2328)

**OUI** Organizationally Unique Identifier (used in MAC addressing).

## P

**Packet** The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

**PAP** Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (*See* CHAP).

**PDU** Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both protocol control information and user data. PDU is sometimes used as a synonym for "packet".

**PEAP** PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See* also EAP-TLS).

**PHP server** Hypertext Preprocessor

**PKI** Public Key Infrastructure

## P (Continued)

- PoE** Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.
- POST** Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.
- push-to-talk (PTT)** The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic.
- A PTT call is initiated by selecting a channel and pressing the “talk” key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.

## Q

- QoS** Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network.
- Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)

## R

- RADIUS** Remote Authentication Dial-In User Service. An authentication and accounting system that checks User Name and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).
- RF** Radio Frequency, a frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF) -- 0-3 Hz to Extremely high frequency (EHF) -- 30GHz - 300 GHz. The middle ranges are: Low frequency (LF) -- 30 kHz - 300 kHz, Medium frequency (MF) -- 300 kHz - 3 MHz, High frequency (HF) -- 3MHz - 30 MHz, Very high frequency (VHF) -- 30 MHz - 300 MHz, Ultra-high frequency (UHF)-- 300MHz - 3 GHz.

## R (Continued)

<b>RFC</b>	Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: <a href="http://www.ietf.org/rfc.html">www.ietf.org/rfc.html</a> .
<b>Roaming</b>	In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.
<b>RP-SMA</b>	Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas
<b>RSN</b>	Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).
<b>RSSI</b>	RSSI received signal strength indication (in 802.11 standard)
<b>RTS / CTS</b>	RTS request to send, CTS clear to send (in 802.11 standard)

## S

<b>Segment</b>	In Ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.
<b>SLP</b>	<p>Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices.</p> <p>With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request.</p> <p>For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent.</p> <p>(SLP version 2, RFC2608, updating RFC2165)</p>
<b>SMI</b>	Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).

## S (Continued)

- SMT (802.11)** Station Management. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are:
- dot11smt - objects related to station management and local configuration
  - dot11mac - objects that report/configure on the status of various MAC parameters
  - dot11res - Objects that describe available resources
  - dot11phy - Objects that report on various physical items.
- SNMP** Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.
- SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.
- SNMP trap** An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).
- SSH** Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
- SSID** Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS.
- In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID.
- Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.



## S (Continued)

<b>SSL</b>	<p>Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URLs that require an SSL connection start with https: instead of http.</p> <p>SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.</p> <p>SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.</p>
<b>Subnet mask</b>	<p>(See netmask)</p>
<b>Subnets</b>	<p>Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.</p>
<b>SVP</b>	<p>SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points in order to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.</p>
<b>Switch</b>	<p>In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.</p>
<b>syslog</b>	<p>A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.</p> <p>Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)</p>

## T

<b>TCP / IP</b>	<p>Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination.</p> <p>TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.</p>
<b>TFTP</b>	<p>Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.</p>
<b>TKIP</b>	<p>Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIPs' enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).</p>
<b>TLS</b>	<p>Transport Layer Security. (See EAP, Extensible Authentication Protocol)</p>
<b>ToS / DSCP</b>	<p>ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service (QoS) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.</p>
<b>TSN</b>	<p>Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1x authentication with Extensible Authentication Protocol (EAP).</p>
<b>Tunnelling</b>	<p>Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.</p>

## U

- UDP** User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.
- U-NII** Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.
- URL** Uniform Resource Locator. the unique global address of resources or files on the World Wide Web. The URL contains the name of the protocol to be used to access the file resource, the IP address or the domain name of the computer where the resource is located, and a pathname -- a hierarchical description that specifies the location of a file in that computer.

## V

- VoIP** Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.
- VPN** Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
- VSA** Vendor Specific Attribute, an attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.

## W

- Walled Garden** A restricted subset of network content that wireless devices can access.
- WEP** Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
- Wi-Fi** Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.

## W (Continued)

- WINS** Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.
- DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
- WLAN** Wireless Local Area Network.
- WM-AD** WM Access Domain Services (WM-AD). Extreme Networks' means of mapping wireless networks to the topology of an existing wired network. When you set up WM-AD on the Summit WM series switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM series switch acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM series switch, one or more Altitude APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM series switch's DHCP server to assign to wireless devices.
- WMM** Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e Quality of Service (QoS) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.
- WPA** Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEPs' basic encryption. For authentication, WPA specifies IEEE 802.1x authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1X for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael.
- WPA requires that all computers and devices have WPA software.

## W (Continued)

### WPA-PSK

Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the Altitude AP or router and the WPA clients.

This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

## Summit WM series switch, access points, and WLAN switch software terms and abbreviations

Term	Explanation
<b>Altitude AP</b>	The Altitude AP is a wireless LAN thin access point (IEEE 802.11) provided with unique software that allows it to communicate only with a Summit WM series switch. (A thin access point handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Altitude AP also provides local processing such as encryption. The Altitude AP is a dual-band access point, with both 802.11a and 802.11b/g radios.
<b>CTP</b>	<p>CAPWAP Tunnelling Protocol (CTP). The Altitude AP uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the 802.11 packets and forward them to the Summit WM series switch.</p> <p>The CTP protocol defines a mechanism for the control and provisioning of Altitude APs (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.</p>
<b>Data Collector</b>	The Data Collector is an application on the Summit WM series switch that receives and manages the Radio Frequency (RF) scan messages sent by the Altitude AP. This application is part of the Summit spy technique, working in conjunction with the scanner mechanism and the Analysis Engine to assist in detecting rogue access points.
<b>DRM (dynamic radio/RF management)</b>	The DRM feature consists of software on the Altitude AP that provides dynamic radio frequency (RF) management. For Altitude APs with the DRM feature enabled and on a common channel, the power levels will be adjusted to balance coverage if an Altitude AP is added to, or leaves, the network. The feature also allows wireless clients to be moved to another Altitude AP if the load is too high. The feature can also be set to scan automatically for a channel, using a channel selection algorithm.

<b>Langley</b>	Langley is a Summit WM series switch, access points, and WLAN switch software term for the inter-process messaging infrastructure on the Summit WM series switch.
<b>Mobility manager (and mobility agent)</b>	<p>The technique in Summit WM series switch, access points, and WLAN switch software by which multiple Summit WM series switches on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM series switches, to provide mobility to the wireless device user.</p> <p>One Summit WM series switch on the network must be designated as the mobility manager. All other Summit WM series switches are designated as mobility agents. Relying on SLP, the mobility manager registers with the Directory Agent and the mobility agents discover the location of the mobility manager.</p>
<b>Summit WM series switch</b>	The Summit WM series switch is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both Altitude APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
<b>Summit spy</b>	The Summit spy is a mechanism that assists in the detection of rogue access points. The feature has three components: (1) a radio frequency (RF) scanning task that runs on the Altitude AP, (2) an application called the Data Collector on the Summit WM series switch that receives and manages the RF scan messages sent by the Altitude AP, (3) an Analysis Engine on the Summit WM series switch that processes the scan data.
<b>WM-AD</b>	WM Access Domain Services (WM-AD). Extreme Networks' means of mapping wireless networks to the topology of an existing wired network. When you set up WM-AD on the Summit WM series switch, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM series switch acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM series switch, one or more Altitude APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM series switch's DHCP server to assign to wireless devices.

## A System states and LEDs

### Summit WM series switch system states and LEDs

The Summit WM series switch has the two system states: Standby and Active.

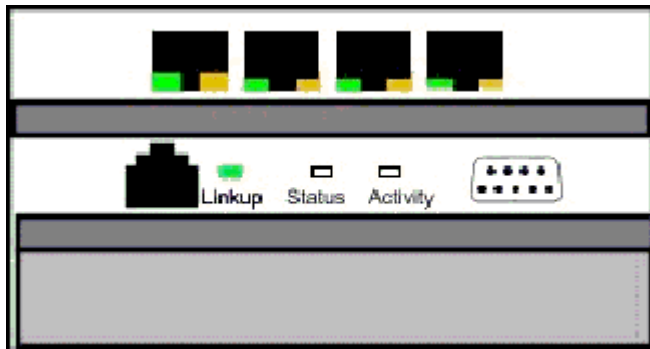
It enters Standby state when shut down in the user interface. During this state, the Summit WM series switch:

- sends a control message to Altitude APs to enter Standby state
- does not handle any wireless traffic or sessions
- disables DHCP, Policy Manager, Security Manager, Altitude AP Manager, and Redirector
- remains on the wired network

The Summit WM series switch enters Active state on startup in the user interface. It responds to the Altitude AP's discover message by returning a message indicating that the Altitude AP can enter the active state.

### Activity and traffic monitoring

The activity and traffic on the Summit WM series switch is monitored via three LEDs on the back of the Summit WM series switch. These LEDs are Link, Status, and Activity.



The three LEDs perform the following functions:

- **Link LED:** Displays the link status of management port Ethernet link as seen by the system software. This LED is only visible at the back of the Summit WM series switch
- **Status LED:** Indicates the state of the controller from software point of view, normal operation, whether processes have gone down, are restarting, and so on. This LED is visible from both the front and the back of the Summit WM series switch.
- **Activity LED:** Indicates the amount of traffic carried to and from Altitude APs. This LED is visible from both the front and the back of the Summit WM series switch.

Table 18 shows the sequence of the Status and Activity LEDs.

**Table 18: Status and Activity LED sequence**

System State	Status LED	Activity LED
Power up	Off	Off
Services started: WDTSTAT installed (init.d starts services)	Blinking Amber	Off
Startup Manager Task started	Solid Amber	Blinking Amber
Startup Manager Task completes startup – all components started	Solid Green	Blinking green, if traffic Blank, if no traffic
A component fails to start or needs restarting (Startup Manager Task retrying that component)	Solid Amber	Blinking green
Summit WM series switch fails to boot	Solid Red	Off
A component fails (no more retries)	Solid Red	Off
System about to be reset by watchdog	Blinking Red	Off

## Altitude AP system states

For the Altitude AP, the Status LED in the center also indicates power. The Status LED is dark when unit is off and is green (solid) when the AP has completed discovery and is operational.

The chart below shows states and corresponding Status LED displays:

**Table 19: Altitude AP system states and status LED displays**

State / Process	Description	LEDs
Power	Altitude AP not powered.	Off
Power	Start up: Power On Self Test (POST)	Steady green (briefly)
Power	Power On Self Test (POST) successful	Off (briefly)
Discovery	If the POST self test is successful, the AP begins Discovery process. Altitude AP is powered on and searching for an active Summit WM series switch. It sends a discover message and waits for a response	Orange (steady)
Fail to find DHCP	Altitude AP failed to find DHCP (will stay in this state until a route appears).	Red-orange (alternate blink)
Failed discovery	If there are SLP issues in failed discovery, the LED display changes.	Green-orange (alternate blink)
Registration	Altitude AP learns the Summit WM series switch's IP address, and can begin the Registration process	Orange (blink)
Failed Registration	Altitude AP fails to learn the Summit WM series switch's IP address.	Red (blink)
Standby	<ol style="list-style-type: none"> <li>Altitude AP enters this state from Discovery when it encounters an active Summit WM series switch and completes the Registration process.</li> <li>Altitude AP enters this state from Active when it receives a control message from the Summit WM series switch to enter this state. If the Altitude AP has any wireless device traffic, it will drop the traffic.</li> </ol>	Green (blink)
	Altitude AP fails to register. It will wait 5 seconds and try again.	Red (slow blink)
	Firmware download from the Summit WM series switch is in progress	Orange + green (blink)



**Table 19: Altitude AP system states and status LED displays (Continued)**

State / Process	Description	LEDs
Active (Ready)	Altitude AP has received a control message from an active Summit WM series switch to enter active or ready state. It is ready to receive wireless traffic. Note: The two Traffic LEDs on either side of the Status LED display a green (blink) if there is active wireless traffic. The left LED is for the 2.4 GHz radio. The right LED is for the 5 GHz radio.	Green (steady)
Vulnerable time interval	Vulnerable time interval (the Summit WM series switch resets to factory default if powered-off for three consecutive times during this state). No vulnerable period when access point is resetting to factory defaults.	Left: Green/Off Center: Off/Green Right: Green/Off
Upgrading firmware	Altitude AP is upgrading its firmware	Center: Red/Green



## B

# Regulatory Information

This section provides the regulatory information for the Summit WM 200/2000 series switch and Altitude 350-2 Access Point.

Configuration of the Altitude 350-2 frequencies and power output are controlled by the regional software purchased with the Summit WM series switch and are downloaded from the sever upon initial set-up. A company is only allowed to download the software related it it's geographic location, thus allowing the proper set-up of Access points in accordance with local laws and regulation. The Altitude 350-2 AP must not be operated until proper regional software is downloaded and properly configured.



### NOTE

Please refer to <http://www.extremenetworks.com/go/rfcertification.htm> for latest regulatory information regarding operation of the Altitude 350-2 Access Point.

*Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that should be performed only by Extreme Networks personnel are clearly identified in this guide.*

*Changes or modifications made to the Summit WM series switch or the Altitude APs which are not expressly approved by Extreme and party responsible for compliance upon installation could void the user's authority to operate the equipment.*

*If agency verification testing is required, contact Extreme Networks for additional instructions.*

## Summit WM200 (15955), Summit WM2000 (15956)

### Safety Standards

North American Safety of ITE:

- UL 60950-1:2003 1st Ed., Listed Device (US)
- CSA 22.2#60950-1-03 1st Ed. (Canada)

European Safety of ITE:

- EN60950-1:2001+A11
- TUV-R GS Mark by German Notified Body
- 73/23/EEC Low Voltage Directive

International Safety of ITE:

- CB Report & Certificate per IEC 60950-1:2001+ Country Deviations
- AS/NZX 3260 (Australia /New Zealand)

## EMI/EMC Standards

North America EMC for ITE:

- FCC CFR 47 part 15 Class A (USA)
- ICES-003 Class A (Canada)

European EMC standards

- EN 55022:1998 Class A
- EN 55024:1998 Class A  
includes IEC 61000-4-2, 3, 4, 5, 6, 11
- EN 61000-3-2,3 (Harmonics & Flicker)
- ETSI EN 300 386:2001 (EMC Telecommunications)
- 89/336/EEC EMC Directive

International EMC Certifications:

- CISPR 22:1997 Class A (International Emissions)
- CISPR 24:1997 Class A (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge, 8kV Contact, 15kV Air, Criteria A
- IEC/EN 61000-4-3 Radiated Immunity 10V/m, Criteria A
- IEC/EN 61000-4-4 Transient Burst, 1kV, Criteria A
- IEC/EN 61000-4-5 Surge, 2kV L-L, 2kV L-G, Level 3, Criteria A
- IEC/EN 61000-4-6 Conducted Immunity, 0.15-80MHz, 10V/m unmod. RMS, Criteria A
- IEC/EN 61000-4-11 Power Dips & Interruptions, >30%, 25 periods, Criteria C

Country Specific:

- VCCI Class A (Japan Emissions)
- AS/NZS 3548 ACA (Australia Emissions)
- CNS 13438:1997 Class A (BSMI-Taiwan)
- NOM/NYCE (Mexico)
- ANATEL (Brazil)
- Argentina Form B
- MIC Mark, EMC Approval (Korea)

## Telecom Standards

- ETSI EN 300 386:2001 (EMC Telecommunications)
- ETSI EN 300 019 (Environmental for Telecommunications)

## Physical and Environmental

### Product Dimensions:

- Width: 17.3 inches (44 cm)
- Depth: 13 inches (33 cm)-with module levers
- Height: 4.4 inches (11.1 cm)-2.5U rack according to IEC 60297-5-100 and IEC 60297-5-107 for front mounted modules

### Product Weight:

- 21 lbs (9.4 kg)-with dual PSU

### Package Dimensions:

- Width: 25.2 inches (63.5 cm)
- Depth: 18.1 inches (46 cm)
- Height: 9.4 inches (24 cm)

### Package Weight:

- 27 lbs (12.3 kg)

## Environmental Operating Conditions for Summit WM100/1000, Summit WM200/2000, and Altitude 350-2 AP

### Environmental Standards:

- EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) - Acoustic Noise
- ASTM D3580 Random Vibration Unpackaged 1.5G

### Operational Environment:

- Operating Temperature Range. 0 C to +40 C (32° F to 104° F)
- Operating Relative Humidity<sup>1</sup> 10 - 90% RH
- Operating Altitude 0 – 3000 meters (9,850 ft)
- Operating Shock (In Rack)<sup>1</sup> 3G, 11ms, 60 shocks
- Operational Office Vibration (In Rack)<sup>1</sup> 5-100-5 Hz @ 2/10G, 0-Peak, 1 Oct./min.
- Operational Random Vibration<sup>1</sup> 3-500 Hz @ 1.5G rms

---

1. Worst-case operational condition. Not for extended use under this condition.

**Storage & Transportation Environment:**

- Storage & Transportation Temp.Range<sup>1</sup>                      -40° C to +70° C (-40° F to 158° F)
- Storage & Transportation Relative Humidity<sup>1</sup>                10 - 95% RH
- Storage & Transportation Shock<sup>1</sup>                                18G @ 6ms, 600 shocks (package < 50kg)
- Storage & Transportation Random Vib.<sup>1</sup>                        5-20 Hz @ 1.0 ASD w/-3dB/oct. from 20-200 Hz
- Storage & Transportation Packaging Drop<sup>1</sup>                    14 drops min on sides & corners @ 39.4"  
(<15kg box)

## Altitude 350-2 Int. AP (15958) AP, Altitude 350-2 Detach. AP (15939)



The above Altitude 350-2 AP models are Wi-Fi certified for operation in accordance with IEEE 802.11a/b/g. Certification# WFA3822.

**NOTE**

*Operation in the European Community and rest of the world may be dependant on securing local licenses/certifications/regulatory approvals. For details and information on the most recent country-specific requirements for the Altitude 350-2 AP, go to the following website: <http://www.extremenetworks.com/go/rfcertification.htm>.*

## United States - FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the transceiver antenna.
- Increase the distance between the equipment and transceiver.


---

1. Worst-case Storage & Transportation condition.

- Connect the equipment to an outlet on a circuit different from that to which the effected equipment is connected.
- Consult the dealer or an experienced radio/TV technician for suggestion.

This equipment meets the conformance standards listed in [Table 20](#).

**Table 20: USA Conformance Standards**

<b>Safety</b>	<ul style="list-style-type: none"> <li>● UL 60950-1:2001 1st Edition, Listed Accessory</li> </ul>	<ul style="list-style-type: none"> <li>● UL 2043 Plenum Rated</li> </ul>
<b>EMC</b>	<ul style="list-style-type: none"> <li>● FCC CFR 47 Part 15 Class B</li> </ul>	 FCC ID#: RJF-A3502A
<b>Radio Transceiver</b>	<ul style="list-style-type: none"> <li>● CFR 47 Part 15.247, Class C, 2.4 GHz</li> <li>● CFR 47 Part 15.407, Class C, 5 GHz</li> <li>● CFR 47 Part 15.205, 15.207, 15.209</li> <li>● CFR 47 Part 2.1091, 2.1093</li> <li>● FCC OET No. 65 1997</li> </ul>	Other: <ul style="list-style-type: none"> <li>● IEEE 802.11a (5 Ghz)</li> <li>● IEEE 802.11b/g (2.4 GHz)</li> <li>● IEEE 802.3af</li> <li>● FCC ID: RJF-A3502A</li> </ul>
<b>Environmental</b>	See Environmental Conditions.	



#### NOTE

The Altitude 350-2 AP must be installed and used in strict accordance with the manufacture's instructions as described in this guide and the quick start guide for the device to which Altitude 350-2 AP is connected. Any other installation or use of the product violates FCC Part 15 regulations.



#### NOTE

Operation of the Altitude 350-2 AP is restricted for indoor use only, in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e).



#### CAUTION

This Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas or other Extreme Networks certified antennas. Any changes or modification to the product not expressly approved by Extreme Networks could void the user's authority to operate this device.

## Conditions Under Which a Second party may replace a Part 15 Unlicensed Antenna

Second party antenna replacement (end user or second manufacturer) is permitted under the conditions listed below, with no testing or filing requirement. The general technical requirement of FCC Part 15.15 (a)(b)(c) still applies, however.

- Replacement antennas must be equal or lower than 4dBi gain within 2.4Ghz range and 5dB gain within 5GHz range. The replacement antenna must be of same type (Omnidirectional Tri band with Reverse SMA connectors) as previously authorized by the Commission/TCB.

- Replacement antennas must be the same pattern type (i.e. similar in-band and out-of-band antenna beam patterns). Special care must be taken when adhering to this condition; the antenna beam patterns of the antennas tested must be compared with the beam patterns of the replacement antennas for similarities.
- Integral and detachable antennas included with the Altitude 350-2 AP models have been tested and included within the FCC/TCB grant. Any other antennas used with the Altitude 350-2 AP models must follow these guidelines to be used legally with the Altitude 350-2 AP.
- Antennas offered for sale by Extreme Networks have been tested using the highest gain of each antenna type at maximum output power.

### FCC RF Radiation Exposure Statement

The Altitude 350-2 Access Point complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.



#### NOTE

---

*The radiated output power of the Altitude 350-2 APs far below the FCC radio frequency exposure limits as specified in “Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields” (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body or other co-located operating antennas.*

### Department of Communications Canada Compliance Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques,” NMB-003 édictée par le ministère des Communications.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This Class B device digital apparatus complies with Canada ICES-003.



This equipment meets the following conformance standards:

**Table 21: Canada Conformance Standards**

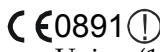
<b>Safety</b>	<ul style="list-style-type: none"> <li>cULus Listed Accessory #60950-1-03 1st edition</li> </ul>	<ul style="list-style-type: none"> <li>Plenum Rated Enclosure</li> </ul>
<b>EMC</b>	<ul style="list-style-type: none"> <li>ICES-003 Class B</li> </ul>	
<b>Radio Transceiver</b>	<ul style="list-style-type: none"> <li>RSS-210</li> <li>RSS-139-1</li> <li>RSS-102 FR Exposure</li> <li>ID# 4141A-3502</li> </ul>	Other: <ul style="list-style-type: none"> <li>IEEE 802.11a (5 GHz)</li> <li>IEEE 802.11b/g (2.4 GHz)</li> <li>IEEE 802.3af</li> </ul>
<b>Environmental</b>	See Environmental Conditions.	

- Operation in the 5150-5250 MHz band is limited to indoor use only to reduce potential for harmful interference to co-channel mobile satellite systems.
- The maximum antenna gain permitted for operation in the 5250-5350 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the external antenna.
- The maximum antenna gain permitted for operation in the 5725-5825 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the external antenna.
- Please note that high power radars are allocated as primary users (meaning they have priority) in the 5250-5350 MHz and 5650-5850 MHz bands and these radars could cause interference and/or damage to LE-LAN devices.

## European Community

The Altitude 350-2 APs are wireless ports designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the wireless port for operation by entry of a country code relative to a specific country. Upon connection to the switch the software will prompt the user to enter a country code. After the country code is entered, the switch will set up the wireless port with the proper frequencies and power outputs for that country code.

## Declaration of Conformity with regard to R&TTE Directive of the European Union 1999/5/EC

The symbol  indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). The Altitude 350-2 Int. AP (15958) and Altitude 350-2 Detach. 15939 models meet the following conformance standards.

**Table 22: European Conformance Standards**

<b>Safety</b>	<ul style="list-style-type: none"> <li>73/23/EEC Low Voltage Directive (LVD)</li> <li>CB Scheme, IEC 60950-1:2001 with all available country deviations</li> </ul>	<ul style="list-style-type: none"> <li>GS Mark, EN 60950-1:2001</li> <li>Plenum Rated Enclosure</li> </ul>
<b>EMC</b>	<ul style="list-style-type: none"> <li>89/336/EEC EMC Directive</li> </ul>	
	<b>Emissions</b>	
	<ul style="list-style-type: none"> <li>EN55022:1998 Class B</li> <li>CISPR22:1997 Class B</li> </ul>	<ul style="list-style-type: none"> <li>EN61000-3-2 and 3-3</li> <li>EN/ETSI 301 489-17 (9-2000)</li> </ul>
	<b>Immunity</b>	
	<ul style="list-style-type: none"> <li>EN55024:1998 Class A, includes IEC 61000-4-2,3,4,5,6,11</li> <li>EN/ETSI 301 489-17 (9-2000)</li> </ul>	
<b>Radio Transceiver</b>	<ul style="list-style-type: none"> <li>R&amp;TTE Directive 1999/5/EC</li> <li>ETSI/EN 300 328-2 2003-04 (2.4 GHz)</li> <li>ETSI/EN 301 893-1 2002-07 (5 GHz)</li> <li>ETSI/EN 301 489-1 2002-08</li> <li>ETSI/EN 301 489-17 2002-08 (RLAN)</li> </ul>	Other: <ul style="list-style-type: none"> <li>IEEE 802.11a (5 GHz)</li> <li>IEEE 802.11b/g (2.4 GHz)</li> <li>IEEE 802.3af</li> </ul>
<b>Environmental</b>	<ul style="list-style-type: none"> <li>EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage</li> <li>EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation</li> <li>EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational</li> <li>ASTM D5276 Drop Packaged</li> <li>ASTM D3580 Random Vibration Unpackaged 1.5 G</li> </ul>	



### NOTE

A signed copy of the Declaration of Conformity (DoC) in accordance with the preceding directives and standards has been made and is available at [www.extremenetworks.com/go/rfcertification.htm](http://www.extremenetworks.com/go/rfcertification.htm).

## Conditions of Use in the European Community

The Altitude 350-2 Access Point with integrated and detachable antennas is designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. If the end user chooses to operate the Altitude 350-2 AP outdoors, it is their responsibility to insure operation in accordance with these rules, frequencies, and power output. The Altitude 350-2 AP must not be operated until proper regional software is downloaded.

**WARNING!**

The user or installer is responsible to ensure that the Altitude 350-2 AP is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the switch to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC. See the switch software guide for detailed instructions on use of this utility.

The Altitude 350-2 Access Point with integrated and detachable antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation for indoor use. These restrictions are described in this section. For the most up to date restriction and limitations go to [www.extremenetworks.com/go/rfcertification.htm](http://www.extremenetworks.com/go/rfcertification.htm).

**NOTE**

The Altitude 350-2 AP is completely configured and managed by the Summit WM series switch connected to the network. Please follow the instructions in this software user guide to properly configure the Altitude 350-2 AP.

- The Altitude 350-2 wireless port requires the end user or installer to properly enter the correct country code into the switch software prior to operating the Altitude 350-2 AP, to allow for proper configuration in conformance with European National spectrum usage laws.
- After the first Altitude 350-2 wireless port is connected to the switch, each additional wireless port connected will inherit the operating configuration of the first Altitude 350-2 wireless port. The user or installer is responsible to ensure the first Altitude 350-2 wireless port is properly configured.
- The software within the switch will automatically limit the allowable channels and output power determined by the current country code entered. Incorrectly entering the country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems.
- This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- The 5 GHz Turbo Mode feature is not enabled for use on the Altitude 350-2 AP Model 15938 and 15939.
- The AutoChannelSelect/SmartSelect setting of the 5 GHz described in the switch software guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements. The current setting for this feature is found in the 5 GHz Radio Configuration Window as described in this switch software manual.
- The Altitude 350-2 AP with integral or detachable antennas may be used to transmit indoors and outdoors in countries of the European Community, as indicated in [Table 23](#). Go to <http://www.extremenetworks.com/go/rfcertification.htm> for the most up to date limitation and restrictions.
- The Altitude 350-2 AP must be operated indoors only when using the 5150- 5350 MHz bands, channels 36, 40, 44, 48, 52, 56, 60, or 64. See [Table 23](#) for permitted 5 GHz channels by country.
- The Altitude 350-2 AP with detachable antenna must be used only with antennas certified by Extreme Networks.
- The Altitude 350-2 AP may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 – 13, except where noted in [Table 23](#).

- In Italy, the end user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium, outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France, outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

## European Spectrum Usage Rules

Table 23 lists the rules and restrictions for operating a 2.4 GHz or 5 GHz device in the European Community. Always use the latest software version for the most up-to-date channel list; some earlier software versions supply only a limited number of channels.

The Altitude 350-2 AP must be installed in the proper indoor or outdoor location. Use the installation utility provided with the switch software to insure proper set-up in accordance with all European spectrum usage rules.

**Table 23: European Spectrum Usage Rules - Effective as of July 2005**

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Belgium <sup>a</sup>	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor <sup>a</sup>
Bulgaria	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Denmark	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Cyprus	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Czech Rep.	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor or Outdoor
Estonia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Finland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
France	Indoor Only	Indoor Only	Expect to Open Fall 2006	Indoor channels 1-13 <b>Outdoor channels 1-7 only</b>
Germany	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Greece	Indoor Only	Indoor Only	Indoor Only	Indoor Only
Hungary	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Iceland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Ireland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Italy	Indoor Only	Indoor Only	Indoor (Outdoor w/License)	Indoor (Outdoor w/License)
Latvia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Liechtenstein	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Lithuania	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Luxembourg	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Netherlands	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Malta	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Norway	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Poland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor

**Table 23: European Spectrum Usage Rules - Effective as of July 2005 (Continued)**

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116,120,124,128,132,136,140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Portugal	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovak Rep.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Slovenia	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Spain	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Sweden	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Switzerland	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
U. K.	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Turbo Mode	Not Allowed in 5GHz	Not Allowed in 5GHz	Not Allowed in 5GHz	Same 2.4 GHz rules as above
AdHoc Mode	Not Allowed	Not Allowed	Not Allowed	Same 2.4 GHz rules as above

- a. Belgium requires that the spectrum agency be notified if you deploy wireless links greater than 300 meters in outdoor public areas using 2.4 GHz band.

## Declarations of Conformity

Table 24 presents the Extreme Networks declarations of conformity for the languages used in the European Community.

**Table 24: Declaration of Conformity in Languages of the European Community**

<b>English</b>	Hereby, Extreme Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
<b>Finnish</b>	Valmistaja Extreme Networks vakuuttaa taten etta Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sita koskevien direktiivin muiden ehtojen mukainen.
<b>Dutch</b>	Hierbij verklaart Extreme Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze verklaart Extreme Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
<b>French</b>	Par la presente Extreme Networks declare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE Par la presente, Extreme Networks declare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
<b>Swedish</b>	Harmed intygar Extreme Networks att denna Radio LAN device star i overensstammelse med de vasentliga egenskapskrav och ovriga relevanta bestammelser som framgar av direktiv 1999/5/EG.
<b>Danish</b>	Undertegnede Extreme Networks erklarer herved, at folgende udstyr Radio LAN device overholder de vasentlige krav og ovrige relevante krav i direktiv 1999/5/EF
<b>German</b>	Hiermit erklart Extreme Networks, dass sich diese Radio LAN device in Ubereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW) Hiermit erklart Extreme Networks die Ubereinstimmung des Gerates Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
<b>Greek</b>	<i>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Extreme Networks ΔΗΛΩΝΕΙ ΟΤΙ Radio LAN device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ</i>
<b>Italian</b>	Con la presente Extreme Networks dichiara che questo Radio LAN device e conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
<b>Spanish</b>	Por medio de la presente Extreme Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
<b>Portuguese</b>	Extreme Networks declara que este Radio LAN device esta conforme com os requisitos essenciais e outras disposicoes da Directiva 1999/5/CE.

## Certifications of Other Countries

The Altitude 350-2 Int. AP (15958) and Altitude 350-2 Detach. AP (15939) APs have been certified for use in the countries listed in [Table 25](#). When the Altitude 350-2 AP is connected to the Extreme Networks switch, the user is prompted to enter a country code. Once the correct country code is entered, the switch automatically sets up the Altitude 350-2 AP with the proper frequencies and power outputs for that country code.


Go to <http://www.extremenetworks.com/go/rfcertification.htm> for the most up to date list of certified countries.



**NOTE**

*It is the responsibility of the end user to enter the proper country code for the country the device will be operated within.*

**Table 25: Other Country Specific Compliance Standards, Approvals and Declarations**

Country	Standards, Approvals, Declarations	
Australia and New Zealand	<ul style="list-style-type: none"> <li>• Altitude 350-2 Int. AP (15958) and Altitude 350-2 Detach. AP (15939) APs</li> <li>• AS/NZS 4288 (Radio)</li> <li>• AS/NZX 3260 (Safety)</li> <li>• AS/NZS 3548 (Emissions)</li> <li>• EEE 802.11a/b/g</li> <li>• IEEE 802.3af (PoE)</li> </ul>	<div style="text-align: center;">                       ACN 090 029 066                 </div> <ul style="list-style-type: none"> <li>• EN 300 328-2:2003-4 (2.4 GHz)</li> <li>• EN 301 893-1:2003-08 (5 GHz)</li> <li>• EN 301 489-17:2002-08 (RLAN)</li> <li>• EN 60950-1:2001 with Australia Deviation</li> </ul>

## Altitude 350-2 Int. AP (15958) and Altitude 350-2 Detach. (15939) Access Points

The Altitude 350-2 AP models are Wi-Fi certified under Certification ID # WFA4279 for operation in accordance with IEEE 802.11a/b/g. The Altitude 350-2 Altitude APs with Internal and External antennas are designed and intended to be used indoors.



**NOTE**

*Operation in the European Community and rest of the world may be dependant on securing local licenses, certifications, and regulatory approvals.*

## Optional Approved 3rd Party External Antennas

The Altitude 350-2 Detach. AP (15939) APs can also be used with optional certified external antennas.

## Antenna Diversity

There are some limitations for using different antennas and Tx/Rx diversity:

- If **Alternate** antenna diversity is used for Tx or Rx, then the same antenna model must be used as left and right antennas. In addition, if cables are used to connect external antennas, the cables must be of the same length and similar attenuation. If these rules are not respected, antenna diversity will not function properly and there will be degradation in the link budget in both directions.
- You can choose to install only one antenna provided that both Tx and Rx diversity are configured to use that antenna and only that antenna. You can choose to install one antenna for 11b/g band and one antenna for 11a band, provided that the antenna diversity is configured appropriately on both radios.

## Sensor Support

Changing the antenna on sensors is not supported (at this stage) for the following reasons:

- The sensor factors the antenna gain and pattern in its calculations and therefore it needs to know the antenna type and gain.
- The sensor operating in mitigation mode becomes a transmitter and must obey the same CTLs as the normal AP software.

## Optional 3rd Party External Antennas for the United States

The Altitude 350-2 Detach. AP (15939) APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested and approved for use with the External Antenna model.



### CAUTION

*When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to these tables.*

## Professional Installation

This device must be professionally installed. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)
- The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.



**Table 26: List of FCC Approved Antennas**

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type
Cushcraft							
# 1	SR2405135Dxxxxx	indoor	Directional	5	2400-2500	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
# 2	S24493DSxxxxx	indoor	Omni, 2 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.
# 3	SL24513Px xxxxx	indoor	Omni	3	2400-2500 5150-5350	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
# 4	S24497Pxxx xxx	indoor	Directional	7	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
Hyperlink Tech							
# 5	HG2458CUX xx	indoor	Omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female
Maxrad							
# 6	MDO24005 PTxxxxxx	indoor	Omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.

**NOTE**

The qualification testing and results are based on above described antennas, cable types, lengths, and connector types. Other cable lengths and connector types are also available which are specified by the suffix part of the part numbers (for example, SR2405135Dxxxxx, where the xxxxxx suffix represents cable length and/or connector type). The antenna feedline used in testing are the minimum cable length. Longer cable may be used with losses greater than or equal to the cables used for testing. The maximum power settings must be adjusted according to these tables.

**NOTE**

If one of the following antennas is used, you must select an operating channel (on the Wireless APs configuration screens) and the corresponding allowed max power from the values listed in [Table 27](#). DO NOT select a higher power than the value listed in [Table 27](#).

Table 27: FCC Antenna Channel-Power Information

Antenna	Frequency (MHz)	Ch. No.	Antenna #1	Antenna #2	Antenna #3	Antenna #4	Antenna #5	Antenna #6
			Cushcraft SR240513 5Dxxxxxx	Cushcraft S24493DSx xxxxx	Cushcraft SL24513Px xxxxx	Cushcraft S24497Pxx xxxxx	Hyperlink Tech HG2458CUxxx	Maxrad MD024005P Txxxxxx
			Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2412	1	16	18	17	16	17	17
	2417	2	17	17	17	16	17	17
	2422	3	18	18	18	18	18	18
	2427	4	18	18	18	18	18	18
	2432	5	18	18	18	18	18	18
	2437	6	18	18	18	18	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	18	18	18	18	18	18
	2462	11	18	18	18	18	18	18
11g	2412	1	10	13	13	10	12	13
	2417	2	14	15	15	14	15	14
	2422	3	15	16	16	15	16	16
	2427	4	16	18	18	16	17	17
	2432	5	16	18	18	17	18	18
	2437	6	16	18	18	17	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	17	17	17	17	17	18
	2462	11	14	14	14	14	14	14

**Table 27: FCC Antenna Channel-Power Information**

Antenna	Frequency (MHz)	Ch. No.	Antenna #1	Antenna #2	Antenna #3	Antenna #4	Antenna #5	Antenna #6
			Cushcraft SR240513 5Dxxxxxx	Cushcraft S24493DSx xxxx	Cushcraft SL24513Px xxxx	Cushcraft S24497Pxx xxxx	Hyperlink Tech HG2458CUxxx	Maxrad MD024005P Txxxxxx
			Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11a	5180	36	N/S	17	17	17	17	N/S
	5200	40	N/S	17	17	17	17	N/S
	5220	44	N/S	17	17	17	17	N/S
	5240	48	N/S	17	17	17	17	N/S
	5260	52	N/S	18	18	18	18	N/S
	5280	56	N/S	18	18	18	18	N/S
	5300	60	N/S	18	18	18	18	N/S
	5320	64	N/S	18	18	18	18	N/S
	5745	149	N/S	15	N/S	15	15	N/S
	5765	153	N/S	15	N/S	15	15	N/S
	5785	157	N/S	14	N/S	14	14	N/S
	5805	161	N/S	14	N/S	14	14	N/S
5825	165	N/S	14	N/S	14	14	N/S	

**CAUTION**

Channels designated as N/S are not supported by the antenna and must not be selected from the Wireless APs configuration screens.

**CAUTION**

For antenna #3 (Cushcraft SL24513Pxxxxx), do not select the Auto channel selection (on the Wireless APs configuration screens) for the 11a radio. Instead, only select a channel from the listed supported channels in [Table 28](#). Operating on a channel that is NOT supported (N/S) is in violation of the law.

**CAUTION**

If you select the Auto channel selection (on the Wireless APs configuration screens), you must also select the power values listed in [Table 28](#). DO NOT select a higher power than the value listed in [Table 28](#).

**Table 28: Auto Channel Selection**

Antenna	11a (dBm)	11b/g (dBm)
#1	N/S	10
#2	14	13
#3	17	13
#4	14	10
#5	14	12
#6	N/S	13

## RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

## Optional 3rd Party External Antennas for Canada

The Altitude 350-2 Detach. (15939) External Antenna APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested with and approved for use with the External Antenna model.



### CAUTION

*When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to these tables.*

## Professional Installation

This device must be professionally installed. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)

The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.

**Table 29: List of IC (Industry Canada) Approved Antennas**

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type
Cushcraft							
#1	SR2405135Dxxxxx	indoor	Directional	5	2400-2500	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#2	S24493DSxxxxx	indoor	Omni, 2 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.
#3	SL24513Pxxxxxx	indoor	Omni	3	2400-2500 5150-5350	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#4	S24497Pxxx	indoor	Directional	7	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
Hyperlink Tech							
#5	HG2458Cuxx	indoor	Omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female
Maxrad							
#6	MDO24005PTxxxxx	indoor	Omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.

**NOTE**

The qualification testing and results are based on above described antennas, cable types, lengths, and connector types. Other cable lengths and connector types are also available which are specified by the suffix part of the part numbers (ex. SR2405135Dxxxxx, where the xxxxx suffix represents cable length and/or connector type). The antenna feedline used in testing are the minimum cable length. Longer cable may be used with losses greater than or equal to the cables used for testing. The maximum power settings must be adjusted according to these tables.

**NOTE**

If one of the following antenna is used, you must select an operating channel (on the Wireless APs configuration screens) and the corresponding allowed max power from the values listed in [Table 30](#). DO NOT select a higher power than the value listed in [Table 30](#).

Table 30: IC Antenna Channel-Power Information

Antenna	Frequency (MHz)	Ch. No.	Antenna #1 Cushcraft SR2405135D xxxxxx	Antenna #2 Cushcraft S24493DS xxxxxx	Antenna #3 Cushcraft SL24513P xxxxxx	Antenna #4 Cushcraft S24497P xxxxxx	Antenna #5 Hyperlink Tech HG2458CU xxx	Antenna #6 Maxrad MD024005P Txxxxxx
			Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2412	1	16	18	17	16	17	17
	2417	2	17	17	17	16	17	17
	2422	3	18	18	18	18	18	18
	2427	4	18	18	18	18	18	18
	2432	5	18	18	18	18	18	18
	2437	6	18	18	18	18	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	18	18	18	18	18	18
	2462	11	18	18	18	18	18	18
11g	2412	1	10	13	13	10	12	13
	2417	2	14	15	15	14	15	14
	2422	3	15	16	16	15	16	16
	2427	4	16	18	18	16	17	17
	2432	5	16	18	18	17	18	18
	2437	6	16	18	18	17	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	17	17	17	17	17	18
2462	11	14	14	14	14	14	14	

**Table 30: IC Antenna Channel-Power Information**

Antenna	Frequency (MHz)	Ch. No.	Antenna #1 Cushcraft SR2405135D xxxxxx	Antenna #2 Cushcraft S24493DS xxxxxx	Antenna #3 Cushcraft SL24513P xxxxxx	Antenna #4 Cushcraft S24497P xxxxxx	Antenna #5 Hyperlink Tech HG2458CU xxx	Antenna #6 Maxrad MD024005P Txxxxxx
			Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11a	5180	36	N/S	17	17	17	17	N/S
	5200	40	N/S	17	17	17	17	N/S
	5220	44	N/S	17	17	17	17	N/S
	5240	48	N/S	17	17	17	17	N/S
	5260	52	N/S	18	18	18	18	N/S
	5280	56	N/S	18	18	18	18	N/S
	5300	60	N/S	18	18	18	18	N/S
	5320	64	N/S	18	18	18	18	N/S
	5745	149	N/S	15	N/S	15	15	N/S
	5765	153	N/S	15	N/S	15	15	N/S
	5785	157	N/S	14	N/S	14	14	N/S
	5805	161	N/S	14	N/S	14	14	N/S
5825	165	N/S	14	N/S	14	14	N/S	

 **CAUTION**

Channels designated as N/S are not supported by the antenna and must not be selected from the Wireless APs configuration screens.

 **CAUTION**

For antenna #3 (Cushcraft SL24513Pxxxxxx), do not select the Auto channel selection (on the Wireless APs configuration screens) for the 11a radio. Instead, only select a channel from the listed supported channels in [Table 31](#). Operating on a channel that is NOT supported (N/S) is in violation of the law.

 **CAUTION**

If you select the Auto channel selection (on the Wireless APs configuration screens), you must also select the power values listed in [Table 31](#). DO NOT select a higher power than the value listed in [Table 31](#).

**Table 31: Auto Channel Selection**

Antenna	11a (dBm)	11b/g (dBm)
#1	N/S	10
#2	14	13
#3	17	13
#4	14	10
#5	14	12
#6	N/S	13

## RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

## Optional 3rd Party External Antennas the European Community

The Altitude 350-2 Detach. (15939) External Antenna APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested with and approved for use with the External Antenna model.



### CAUTION

*When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to these tables.*

## Professional Installation

This device must be professionally installed. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)

The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.



**Table 32: Approved Antenna List for Europe**

#	Model	Location	Type	Gain (dBi)	Frequency (MHz)
Huber+Suhner					
#1	SOA 2454/360/7/20/DF	outdoor-capable	Omni	6 8	2400-2500 4900-5875
#2	SPA 2456/75/9/0/DF	outdoor-capable	Planar 2 or 1 inputs	9	2400-2500 5150-5875
#3	SPA 2400/80/9/0/DS	outdoor-capable	Planar 2 inputs	8.5	2300-2500
#4	SWA 0859/360/4/10/V	outdoor-capable	Omni	7	2400-5875
#5	SOA 2400/360/4/0/DS	outdoor-capable	Omni	3.5	2400-2500
#6	SPA 2400/40/14/0/DS	outdoor-capable	Planar 2 inputs	13.5	2400-2500
#7	SWA 2459/360/4/45/V	outdoor-capable	Omni	>4	2400-5875

**NOTE**

If one of the following antenna is used, you must select an operating channel (on the Wireless APs configuration screens) and the corresponding allowed max power from the values listed in [Table 33](#). DO NOT select a higher power than the value listed in [Table 33](#).

Table 33: ETSI Antenna Channel-Power Information

Antenna	Frequency (MHz)	Ch. No.	Antenna #1	Antenna #2	Antenna #3	Antenna #4	Antenna #5	Antenna #6	Antenna #7
			Huber +Suhner SOA 2454/360/7/20/DF	Huber +Suhner SPA 2456/75/9/0/DF	Huber +Suhner SPA 2400/80/9/0/DS	Huber +Suhner SWA 0859/360/4/10/V	Huber +Suhner SOA 2400/360/4/0/DS	Huber +Suhner SPA 2400/40/14/0/DS	Huber +Suhner SWA 2459/360/4/45/V
			Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2412	1	15	14	14	15	15	9	15
	2417	2	15	14	14	15	15	9	15
	2422	3	15	14	14	15	15	9	15
	2427	4	15	14	14	15	15	9	15
	2432	5	15	14	14	15	15	9	15
	2437	6	15	14	14	15	15	9	15
	2442	7	15	14	14	15	15	9	15
	2447	8	15	14	14	15	15	9	15
	2452	9	15	14	14	15	15	9	15
	2457	10	15	14	14	15	15	9	15
	2462	11	15	14	14	15	15	9	15
	2467	12	15	14	14	15	15	9	15
	2472	13	15	14	15	15	15	10	15
11g	2412	1	15	13	14	15	15	9	15
	2417	2	15	13	14	15	15	9	15
	2422	3	15	13	14	15	15	9	15
	2427	4	15	13	14	15	15	9	15
	2432	5	15	13	14	15	15	9	15
	2437	6	15	13	14	15	15	9	15
	2442	7	15	14	14	15	15	10	15
	2447	8	15	14	14	15	15	10	15
	2452	9	15	14	14	15	15	10	15
	2457	10	15	14	14	15	15	10	15
	2462	11	15	14	14	15	15	10	15
	2467	12	15	14	14	15	15	10	15
	2472	13	15	13	13	15	15	9	15

**Table 33: ETSI Antenna Channel-Power Information**

Antenna	Frequency (MHz)	Ch. No.	Antenna #1 Huber +Suhner SOA 2454/ 360/7/20/ DF Power limit (dBm)	Antenna #2 Huber +Suhner SPA 2456/75/ 9/0/DF Power limit (dBm)	Antenna #3 Huber +Suhner SPA 2400/ 80/9/0/DS Power limit (dBm)	Antenna #4 Huber +Suhner SWA 0859/ 360/4/10/ V Power limit (dBm)	Antenna #5 Huber +Suhner SOA 2400/ 360/4/0/ DS Power limit (dBm)	Antenna #6 Huber +Suhner SPA 2400/ 40/14/0/DS Power limit (dBm)	Antenna #7 Huber +Suhner SWA 2459/ 360/4/45/V Power limit (dBm)
	11a	5180	36	16	16	N/S	16	N/S	N/S
5200		40	16	16	N/S	16	N/S	N/S	16
5200		44	16	16	N/S	16	N/S	N/S	16
5240		48	16	16	N/S	16	N/S	N/S	16
5260		52	16	16	N/S	16	N/S	N/S	16
5280		56	16	16	N/S	16	N/S	N/S	16
5300		60	16	16	N/S	16	N/S	N/S	16
5320		64	16	16	N/S	16	N/S	N/S	16
5500		100	20	19	N/S	20	N/S	N/S	20
5520		104	20	19	N/S	20	N/S	N/S	20
5540		108	20	19	N/S	20	N/S	N/S	20
5560		112	20	19	N/S	20	N/S	N/S	20
5580		116	20	19	N/S	20	N/S	N/S	20
5600		120	20	19	N/S	20	N/S	N/S	20
5620		124	20	19	N/S	20	N/S	N/S	20
5640		128	20	19	N/S	20	N/S	N/S	20
5660		132	20	19	N/S	20	N/S	N/S	20
5680		136	20	19	N/S	20	N/S	N/S	20
5700	140	20	19	N/S	20	N/S	N/S	20	

**CAUTION**

Channels designated as N/S are not supported by the antenna and must not be selected from the Wireless APs configuration screens.

**CAUTION**

If you select the Auto channel selection (on the Wireless APs configuration screens), you must also select the power values listed in [Table 34](#). DO NOT select a higher power than the value listed in [Table 34](#).

**Table 34: Auto Channel Selection**

Antenna	11a (dBm)	11b/g (dBm)
#1	16	15
#2	16	13
#3	N/S	13
#4	16	15
#5	N/S	15
#6	N/S	9
#7	16	15

### RF Safety Distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

## A

- accounting
  - setup on a WM-AD, 121
- adding
  - Altitude AP manually, 63
- alarms
  - overview of log types and levels, 220
- allow all or approved APs
  - for availability setup, 155
- allow or deny in a filtering rule, 91
- Altitude AP
  - adding for availability setup, 155
  - adding manually, 63
  - assigning to a WM-AD, 107
  - client disassociate, 203
  - default configuration, 30, 35, 58, 66, 68, 79, 153, 155, 159
    - copy to defaults, 79
  - international licensing, 56
  - LED sequence in discovery, 58
  - maintenance and reboot, 81
  - radios, 56, 70
  - static configuration, 75
  - view statistics, 193
- Analysis engine
  - functions, 183
- antennae on the Altitude AP, 56
- authentication
  - MAC-based, 119
  - no RADIUS server, 87
  - none on a WM-AD, 142
  - on a WM-AD for AAA, 116
  - on a WM-AD for Captive Portal, 109
  - overview of types, 108
  - protocols supported, 89, 112
- Authentication, Authorization, Accounting (AAA)
  - filter ID values (RADIUS policy), groups, 122
  - set up 802.1x authentication, 116
  - set up privacy on a WM-AD, 138
- availability, 155

## B

- backup controller software configuration, 214
- branch office, static configuration of Altitude AP, 75

## C

- call data records (CDRs), 121
- Captive Portal
  - authentication on a WM-AD, 109
  - configuring internal, external Captive Portal, 114
  - defined, 89
  - non-authenticated filtering rules, 126
  - privacy mechanisms, 135
  - set up a WM-AD topology, 98
  - view sample page, 115
- Check Point event logging, 167
- configuring
  - Captive Portal, internal, external, 114
  - software - overview steps, 30
  - static routes, 45
- controller
  - availability overview, 29
  - back up software configuration, 214
  - define management user names, passwords, 163
  - define network time synchronization, 165
  - defined as mobility manager for mobility, 159
  - enable ELA event logging (Check Point), 167
  - events during a failover, 158
  - paired for availability, 153
  - restore software configuration, 217
  - set up third-party APs, 175
  - system maintenance, 208
  - system shutdown, 208

## D

- default filter, 131
- default gateway on a WM-AD, 102
- disassociate a wireless client, 203
- discovery
  - Altitude AP LED sequence, 58
  - steps, 57
- displays
  - Altitude AP availability, 156, 193
  - Altitude AP wired and wireless statistics, 193
  - client location by foreign Summit switch, 163, 196
  - client location by home, 163, 196
  - list of displays, 191
  - Summit switch tunnel traffic, 163, 196

- documentation feedback, 10
- Domain Name Server (DNS)
  - in discovery, 57
- DSCP classifications, 147
- Dynamic Host Configuration Protocol (DHCP)
  - for availability, 153
  - for mobility (WM Access Domain Manager), 159
  - Option 78 in discovery, 57
  - relay on a WM-AD, 104
  - required as part of solution, 22

## E

- event logging
  - in Check Point, 167
  - in Summit switch software, 220
- exception filters
  - on a WM-AD, 124
  - port-based, 51
- exclusions, IP address range on a WM-AD, 103

## F

- failover of a controller
  - availability overview, 29
  - events and recovery, 158
- failover of a RADIUS server, 112
- filtering
  - default filter, 131
  - exception filter on a WM-AD, 124
  - filtering rules, overview of set up, 123
  - for an AAA group, 133
  - for Captive Portal authentication, 115
  - non-authenticated filter for Captive Portal, 126
  - non-authenticated filtering rules, examples, 128
  - on a WM-AD for third-party APs, 177
  - overview of packet filtering, 28
  - overview, four types, 90
  - port-based, 50
  - rules for filter ID values, 129
  - set filter ID values (RADIUS policy), 122
- formatting conventions, 10
- forwarding table report, 47

## G

- gateway, default, on a WM-AD, 102
- global settings
  - for a WM-AD, 92
  - RADIUS servers for authentication, 111, 118, 120, 122

- groups for Authentication, Authorization, Accounting (AAA), 122

## H

- health checking status of Altitude APs, 208
- heartbeat messages, in WM Access Domain Manager feature, 159

## I

- IP address range on a WM-AD, 103

## L

- LED sequence
  - in discovery, 58
- login user name and password, 37
- Login-LAT-Group, 129
  - for WM-AD AAA authentication, 122
- logs
  - changing log level, 208
  - event logging in Check Point, 167
  - overview of types and levels, 220

## M

- MAC-based authentication, 119
- Management Information Bases (MIBs) supported, 169
- management port
  - management traffic on data port, 45
  - modify management port settings, 40
  - port-based filtering, 50
- management traffic
  - enabling on a WM-AD, 100
- mobility
  - mobility manager and mobility agent, 159
  - overview, 29
- mobility manager
  - defining a controller for mobility, 159
- multicast
  - for a WM-AD, 133

## N

- network assignment
  - by AAA, 138
  - by SSID for Captive Portal, 98
  - options for a WM-AD, 87
  - VLAN, 23, 26
- network time synchronization, 165
- next hop route for a WM-AD, 101
- non-authenticated filter for Captive Portal, 115, 126

**O**

- operating system software upgrade, 210
- OSPF
  - configuring, 47
  - linkstate report, 50
  - neighbor report, 50
  - on a WM-AD, 101
- overview, 28

**P**

- password, for management users, 163
- port
  - port exception filters, 51
- priority override, 144
- privacy
  - dynamic WEP on a WM-AD for AAA, 139
  - encryption methods supported, 27
  - on a WM-AD for AAA
    - AAA, 138
  - overview on a WM-AD, 92
  - setup on a WM-AD for Captive Portal, 135
  - static WEP for an AAA WM-AD, 138
  - WPA v1 and WPA v2 on a WM-AD for AAA, 139
- product key
  - system maintenance, 210
- protocols
  - for authentication by Captive Portal, 112

**Q**

- QoS (Quality of Service), 30, 88, 94, 142, 144, 238, 242
  - admission control thresholds, 94
  - advanced, 147
  - modes, 144
  - policy, 146

**R**

- radio
  - 5 GHz (a) and 2.4 GHz (b/g), 56
  - channels, 70, 74
- radio settings
  - view and modify, 70
- RADIUS server
  - deployment with no server, 87
  - filter ID values, 129
  - for authentication, 111, 118, 120, 122
  - for MAC-based authentication, 119
  - priority for redundancy, 112
  - RADIUS accounting, 121
  - RADIUS policy for a WM-AD, 122
  - required as part of solution, 22

- VSAs in RADIUS message, 108
- random delays, 59
- read/write privileges, 163
- reboot Altitude AP, 81
- registration
  - settings for availability setup, 155
- reports
  - AP inventory, 198
  - forwarding table, 47, 198
  - list of displays, 191
  - OSPF linkstate, 50, 198
  - OSPF neighbor, 50, 198
- restore controller software configuration, 217
- rogue detection, Summit spy feature, 184
- routing
  - configuring OSPF on data port, 47
  - configuring static routes, 45
  - next hop route on a WM-AD, 101
  - overview, 28
- routing table
  - viewing, 47

**S**

- scan results, Summit spy feature, 184
- security of network, overview of methods, 26
- service class, 142
- Service Location Protocol (SLP)
  - for availability, 153
  - for mobility (WM Access Domain Manager), 159
  - in discovery, 57
  - required as part of solution, 22
  - traffic allowed on data port, 45
  - view sldump tool report, 156
- set up for a WM-AD, 175
- shut down system, 208
- Simple Network Management Protocol (SNMP)
  - MIBs supported, 169
- software
  - maintenance of Altitude AP software, 81
  - maintenance of Controller software, 210
- SSID network assignment for Captive Portal, 98
- static configuration of Altitude AP, 75
- static routes
  - configuring, 45
  - viewing forwarding table report, 47
- syslog event reporting
  - define parameters, 208

**T**

- third-party APs, 175
  - defining a WM-AD for, 100

- in Summit spy feature, 188
- topology of a WM-AD
  - Captive Portal, 98
- traces
  - overview of log types and levels, 220
- Type of Service (ToS/DSCP)
  - on a WM-AD, 142
  - Quality of Service, 30

## U

- user name and password for login, 37
- user name and password, changing, 163

## V

- vendor specific attributes (VSA)
  - in RADIUS message, 108
  - RADIUS server
    - vendor specific attributes, 112, 119
- VLAN
  - configuration, 76, 97, 102, 144, 149, 150
  - IDs, 150, 151
- Voice-over-IP (VoIP)
  - define multicast groups on a WM-AD, 133
  - set up a WM-AD for, 142
- vulnerable time interval, 59

## W

- Wi-Fi Multimedia (WMM)
  - on a WM-AD, 142
  - Quality of Service, 30
- Wi-Fi Protected Access (WPA)
  - overview on a WM-AD, 92
  - PSK mode for Captive Portal, 136
  - WPA v1 and v2 on a WM-AD for AAA, 139
- Wired Equivalent Privacy (WEP)
  - on a WM-AD for AAA, 138
  - overview on a WM-AD, 92
  - static for Captive Portal, 135
- WM Access Domain Services (WM-AD), 28
  - authentication by AAA (802.1x), 116
  - authentication by Captive Portal, 109
  - define filtering rules, 123
  - defined, 85
  - for third-party APs, 176
  - global settings, 92
  - multicast, 133
  - network assignment overview, 87
  - privacy for AAA, 138
  - privacy overview, 135
  - set up for VoIP, 142
  - topology for Captive Portal, 98