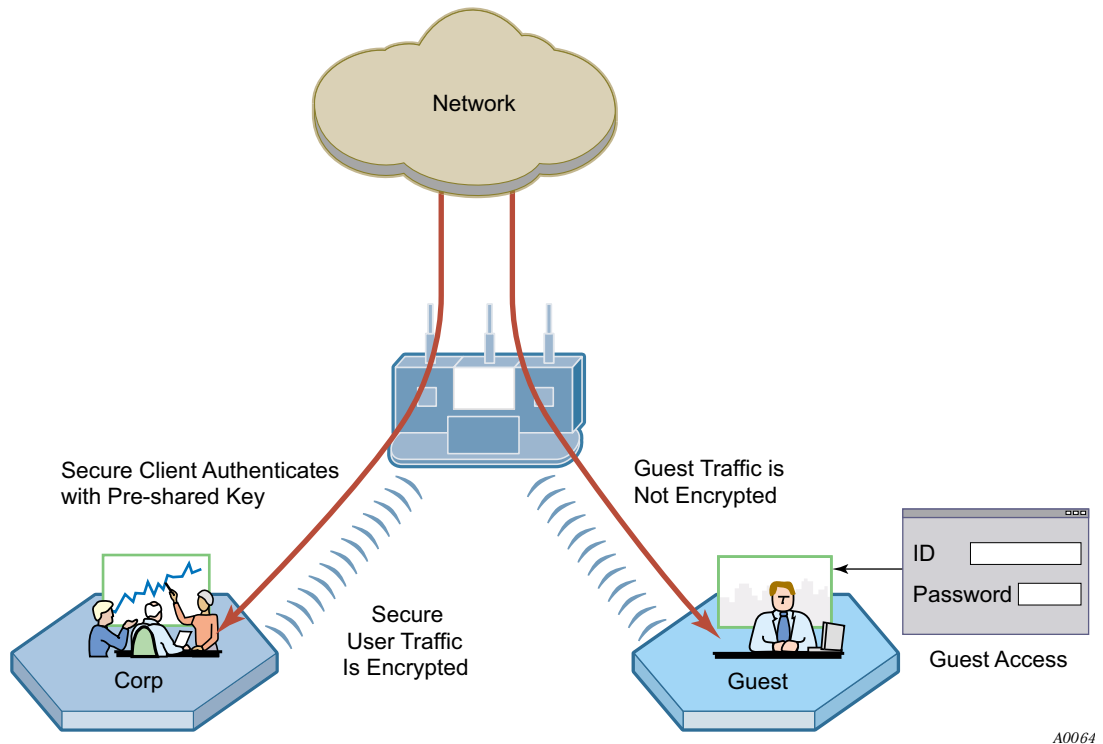


NOTE: If both secured and open access are enabled (mixed-mode of operation) then some third party clients may not be able to access the network using WPA-PSK. All clients will be able to connect to the network using the open authentication correctly.

Figure 119 provides a sample illustration of how clients are treated when guest access is implemented without VLANs. Secure clients are authenticated using WPA-PSK, while guests are authenticated through the landing page (internal page is shown). Both types of users gain access to the same network resources; however, only the secure user traffic is encrypted.

Figure 119: Guest Access Without VLANs



Guest access with VLANs

This option, in which VLANs are used to differentiate between corporate traffic and guest user traffic, is ideal for businesses that want to provide guest access to visitors. When guest users log in, they are automatically assigned to the guest VLAN and are prevented from accessing the main corporate network.

To use VLANs for guest access, the AP must be connected to a VLAN-aware switch, and the switch must be configured to support the designated VLANs. The VLAN configuration of the upstream network should make available only those network resources set aside for guest use. This often means prohibiting guest stations from accessing anything other than the corporate open subnet or the Internet.

For open guest access, the Open access security option must be configured. This precludes the use of WEP Security Mode on APs that provide guest access, but does permit use of WPA Security Mode for non-guests only.

VLANs and security privileges are assigned to users by way of service profiles defined for user groups and bound to the network SSID. It is required that the VLAN configuration include DHCP and DNS services.

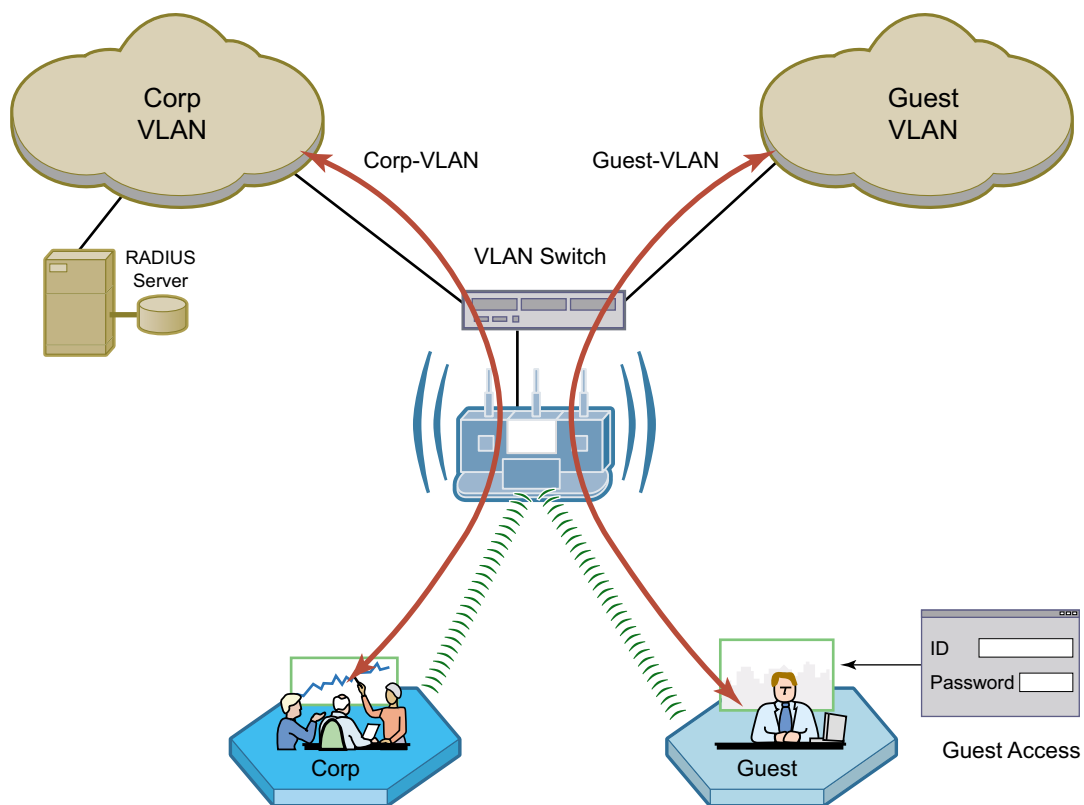


NOTE: If guest access is configured on a VLAN other than VLAN 1, the DHCP server on the AP cannot be used to provide IP address service for the guest VLAN. Use an external DHCP server.

Internal Landing Page

The internal landing page is a configurable option within the Airgo AP. The guest password for the AP can be set using the Guest Access panel, or an automatically generated password can be configured through the User Management panel in NM Portal. If the automatically generated guest password is used, then the authentication process for the internal landing page also checks the password entered by the guest user against the RADIUS authentication service provided in the security portal. If either password is acceptable, the guest user is authenticated and receives the privileges specified in the guest service profile. Internal landing pages are compatible with the VLAN and non-VLAN options.

Figure 120 shows how Acme Works configured guest access with an internal guest landing page. In this example, the company has two VLANs: Corporate and Guest. Corporate and guest users belong to the Enterprise and Guest user groups, respectively, with appropriate service profiles assigned and bound to the SSID. Corporate users are authenticated by way of the enterprise RADIUS server, while guest users are authenticated by way of an internal landing page configured in the Airgo AP. After they are authenticated, guest users are placed in the Guest VLAN.

Figure 120: Guest Access - Internal Landing Page

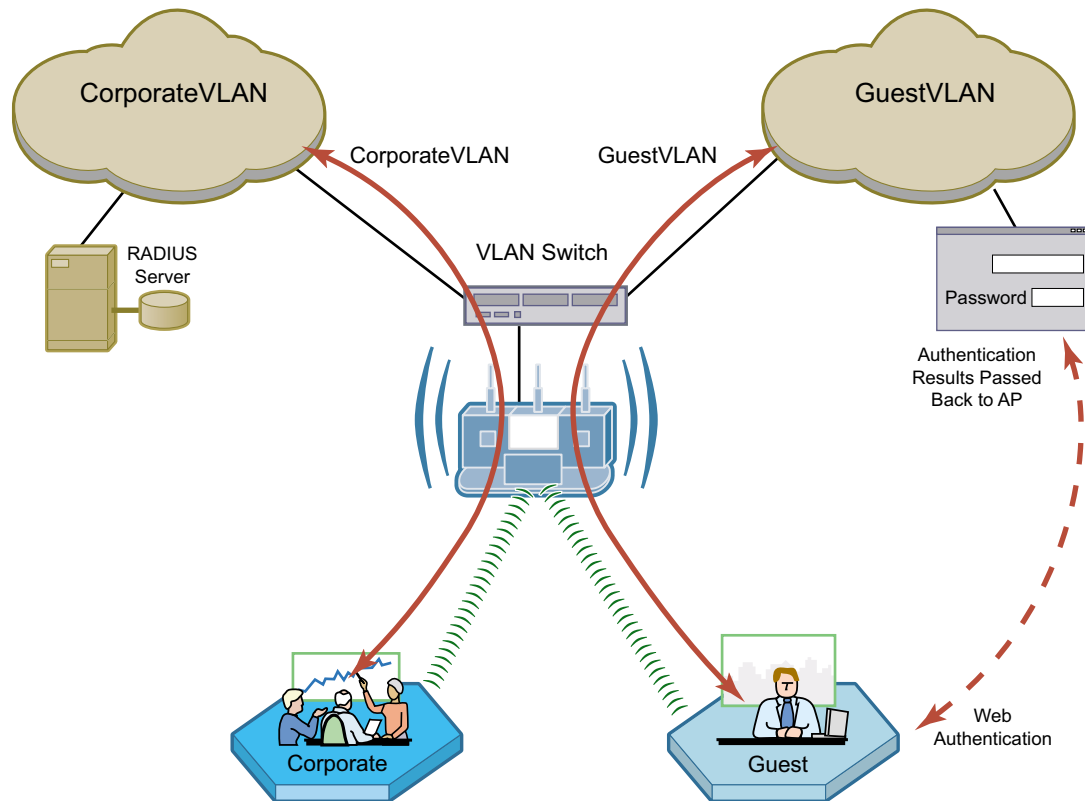
A0045D

External Landing Page

An external landing web page can be set up through a corporate web server. The URL for the landing page must use an IP address rather than a domain name. Regardless of the authentication process selected for the external page, it is necessary to forward authentication results to the AP upon completion of successful or unsuccessful guest authentication.¹ External landing pages are compatible with the VLAN and non-VLAN options.

Figure 121 shows a network VLAN configuration with an external guest landing page. The external landing page is made accessible over the Internet through an external web server. As in the previous example, authenticated guest users are given access to the guest VLAN.

Figure 121: Guest Access - External Landing Page



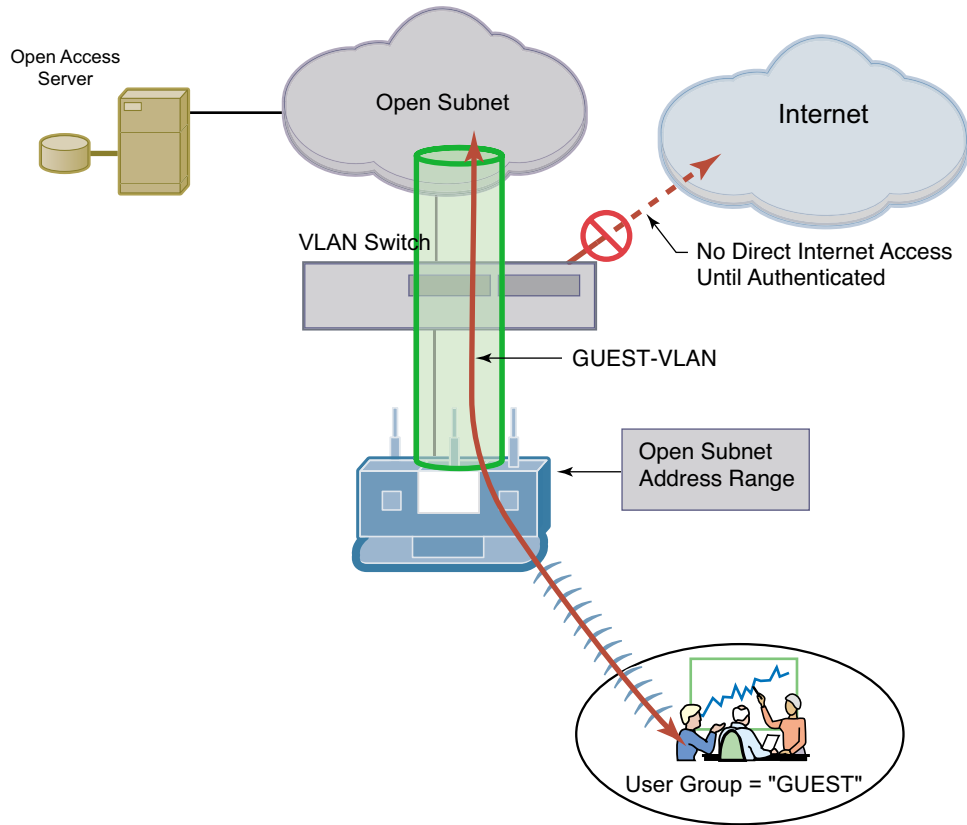
A0045B

¹ An example external landing page is shipped with the Airgo AP.

Open Subnet

In an optional open subnet arrangement, shown in Figure 122, unauthenticated guest users are permitted limited access to an open enterprise subnet specified in the Airgo AP. The enterprise open subnet must be part of the Guest VLAN. Extended access requires authentication through an internal or external landing page.

Figure 122: Guest Access - Open Subnet



A00.35 B

Guest Access Persistence

If a guest user is temporarily disconnected from the Airgo AP due to loss of association, it may not be necessary for the user to reauthenticate if the client reassociates to the same AP within one minute. This is particularly beneficial when using a virtual private network (VPN) with guest access, wherein the user signs on as a guest and then launches a VPN session to a remote VPN server. Since the VPN session is tunneled over the guest session, a temporary loss of connectivity does not require tearing down the VPN session. If loss of association extends beyond one minute, it is necessary for the guest user to reauthenticate.

Configuring Guest Access with VLANs

This section describes the complete process of setting up guest access with VLANs. Use the Guest Access wizard for easy configuration of the major guest access parameters. See “Guest Access Wizard” on page 53 for instructions on using the Guest Access wizard.

Task	Steps
Confirm that Open access is supported as a security option.	1 Choose Wireless Security from the Security Services menu to open the Security Mode tab (“Configuring Wireless Security” on page 150). 2 Enable WPA security if mixed mode security (encrypted and Open) is desired. Only WPA can be enabled in conjunction with Open. The WPA Security mode is for non-guests only. 3 Enable Open Access. 4 Click Apply.
Create or confirm existence of a corporate VLAN. This can be the default untagged VLAN or a specially created VLAN.	1 Choose VLAN Configuration from the Networking Services menu to open the VLAN table (“VLAN Table” on page 112). 2 Confirm that the corporate VLAN is listed in the table, or click Add to create a new VLAN: - a Enter the corporate VLAN name and a numeric VLAN ID in the Add VLAN entry panel. - b Enter the IP address and maskbits of the captive portal server, or select the DHCP option. The guest portal must have a valid IP address for the authentication process to work. - c Select the eth0 interface, and mark it as tagged. (Only eth0 should be tagged.) - d Click Add.
Create the guest VLAN.	1 Choose VLAN Configuration from the Networking Services menu to open the VLAN table (“VLAN Table” on page 112). 2 Click Add. 3 Enter the VLAN name (Guest VLAN) and a numeric VLAN ID in the Add VLAN entry panel. It is not recommended that you use the default VLAN. 4 Enter the IP address and maskbits of the captive portal server, or select the DHCP option. 5 Select the eth0 interface, and mark it as tagged. (Only eth0 should be tagged.) 6 Click Add. For additional information on configuring VLANs, see “Configuring VLANs” on page 111.
Create or confirm definition of a corporate service profile.	1 Choose SSID Configuration from the Wireless Services menu to open the SSID table (“SSIDs and Service Profiles” on page 84). 2 Click Profile Table. 3 Add a corporate profile or confirm that one exists with the desired WPA security option and the corporate VLAN specified. Make sure that the corporate profile is bound to the SSID.

Task (continued)**Steps**

Create a guest service profile which specifies the guest VLAN and desired COS and security options.

- 1 Choose **SSID Configuration** from the **Wireless Services** menu to open the SSID table.
- 2 Select **SSID Details** (“SSID Details” on page 87).
- 3 Confirm the SSID name, or enter a new SSID name for the Guest Portal, and then click **Apply**.
- 4 Click **Profile Table** to display the current list of service profiles.
- 5 Click **Add** to create the guest service profile. Select the VLAN ID for the guest VLAN previously defined. Enter the COS value and make sure that no-encryption is selected.
- 6 Click **Apply**.

Add guest access to the SSID and specify an internal or external landing page for guest users who attempt to access the network.

- 1 Choose **Guest Access Configuration** from the Guest Access Services menu to open the Guest table.
- 2 Click **Add**.
- 3 Confirm selection of the SSID and guest profile, as defined in the previous task.
- 4 Select whether the landing page will be internal or external. If external, enter a URL and an external web server secret code, which is the shared secret code for communication between the AP and web server.
- 5 Click **Apply**.

For the internal landing page, set a guest password; for an external landing page use the RADIUS shared secret code.

- 1 If Internal is selected as the landing page type, click **Security** to enter the guest password.
- 2 Enter and confirm the password, and click **Apply**.

Set up optional auto-generation of guest passwords

- 1 From NM Portal Network Management Explorer window, select **User Management** from the Security Portal menu.
- 2 On the Guest User tab (Figure 126), select **Yes** to enable auto-password generation.
- 3 Select an interval from the Generate Auto Guest Password pull-down list.
- 4 Click **Apply**.

NOTE: If static and auto-generated passwords are configured, then a guest user can enter either password to be authenticated.

Guest access is now configured. When guests attempt to access the network, they are directed to an external landing page or to a standard user login screen. Upon entering the correct guest password or server secret code, they are granted access to the guest VLAN. They are also given the COS and encryption characteristics specified in the guest service profile.

See also “Guest Access Wizard” on page 53.

Guest Access Services Panel

For summary information about guest access, use the Guest Access Configuration panel. The panel opens to the Guest table (Figure 123), which lists currently defined guest service profiles. If guest access is enabled, you can also open the Guest table by clicking the Guest Access Enabled link on

the SSID Details panel. (The panel is described in “SSID Details” on page 87.) The Guest table presents the following information:

Field	Description
SSID	The network to which the guest profile belongs (There can be at most one guest profile per SSID.)
Service-Profile	The name of the guest service profile bound to the SSID.
Landing Page	Internal or external page automatically that automatically opens when guest users attempt to access the network
Allowed Guest Subnet	The subnet optionally reserved for unauthenticated guest access (Configuring an allowed guest subnet can give unauthenticated users access to a limited set of free services.)

Figure 123: Guest Access Configuration - Guest Table

Guest access configuration has the following prerequisites: configuration of a Guest VLAN, configuration of a Service-Profile that references the Guest VLAN and binding of the Service-Profile to the SSID on which guest-access is enabled. Guest access feature allows the use of internal landing page or external landing page. If internal landing page is used, then configure appropriate guest-password security.

Guest Table	SSID	Service-Profile	Landing Page	Allowed Guest Subnet
☐	Corporate	Guest	Internal	

ADD MODIFY DELETE

Perform the following functions from the Guest Table:

Function	Description
Add an entry to the Guest Table	One guest profile can be added for each SSID. If a profile is already assigned to an SSID and you add a new one, it replaces the previously defined profile. 1 Click Add to open the Add Guest to SSID entry panel (Figure 124). 2 Select the SSID. 3 Select the service profile from the Profile pull-down list. The profile details are listed at the bottom of the entry panel. 4 If desired, enter the address and maskbits for a subnet optionally reserved for unauthenticated guest access (A.B.C.D/maskbits format) 5 Select an internal or external landing page. If the external page is selected, enter the full IP-based URL and the shared secret code used for communicating with the RADIUS server. 6 Click Apply.
Modify an entry	1 Select the entry you wish to modify, and click Modify. 2 Confirm the SSID. 3 Select the service profile from the Profile pull-down list. 4 If desired, enter the address and maskbits for a subnet optionally reserved for unauthenticated guest access. 5 Select an internal or external landing page. If the external page is selected, enter the full URL and shared secret code for access. Click Apply.
Delete an entry	6 Select the entry and click Delete. 7 Click OK to confirm.

Figure 124: Guest Access Configuration - Add Guest to SSID

Guest Access Security

The Security tab of the Guest Access Configuration panel (Figure 125) provides an interface to set the guest password for an internal landing page.

Figure 125: Guest Access Configuration - Security

GUEST TABLE **SECURITY** **HELP** **LOGOUT**

Guest Access Services | Guest Access Configuration | Security »

Guest Access can be secured by means of a 'Guest Access Password', which is bound to the 'Internal Landing Page'. A guest user would be required to enter the correct Guest Access Password to gain access to guest services (such as Internet access).

Guest Authentication

Guest Access Password *

Confirm Guest Access Password *

APPLY

Auto-Generating Guest Passwords

For optional generation of guest passwords automatically at set intervals, use the Guest User tab within the security area of NM Portal (Figure 126).

Figure 126: Security Portal - Guest User

WIRELESS USERS **ADMIN USERS** **MAC ACLs** **GUEST USER** **?** **CLOSE**

Security Portal | User Management | Guest User »

Auto Guest Password Generation feature enables auto-generation of Guest-Access password on a Portal AP. All APs managed by this Portal AP, using internal landing page, will use this common password for Guest Access. You can change the frequency of password change. If an admin e-mail address and SMTP server are configured on the Portal AP, then all updates to this password will be communicated via e-mail.

Auto Guest Password Generation

Enable Auto Guest Password Generation ☐ Yes ☒ No

Current Auto Guest Password Generation Time

Generate Auto Guest Password

APPLY **RESET**

Auto Guest Password Details

Current Auto Generated Guest Password

REFRESH

9 Managing the Network

This chapter explains how to use the NM Portal features of the Airgo Access Point to manage multiple APs across the network. It includes the following topics:

- [Introduction](#)
- [Using NM Portal](#)
- [Using the Network Topology Menu](#)
- [Managing Rogue Access Points](#)
- [Using the NM Services Menu](#)
- [Managing Network Faults](#)
- [Using the Security Portal Menu](#)
- [Using the Mobility Services Menu](#)

Introduction

Network management refers to the coordinated control and supervision of multiple access points across a network. Network management functions include single-point configuration of multiple access points, user access control, performance monitoring, and fault management.

A unique network management capability is built into the Airgo Access Point. When configured as an NM Portal, the Airgo AP can provide network management services for up to five subnetworks. For small-size to mid-size networks, this eliminates the need for an external network management application. For mid-size to large-size enterprise networks, NM Portal can manage all the APs at a specific location or branch, while NMS Pro, offered as a separate product, can supply enterprise-level network management.

NM Portal supports the following functions:

- Single view to manage the entire network
- AP discovery
- AP enrollment
- Centralized software distribution and policy management
- Integrated security management for users
- Rogue AP control
- Email alerts
- Fault management
- Syslog
- Guest access control

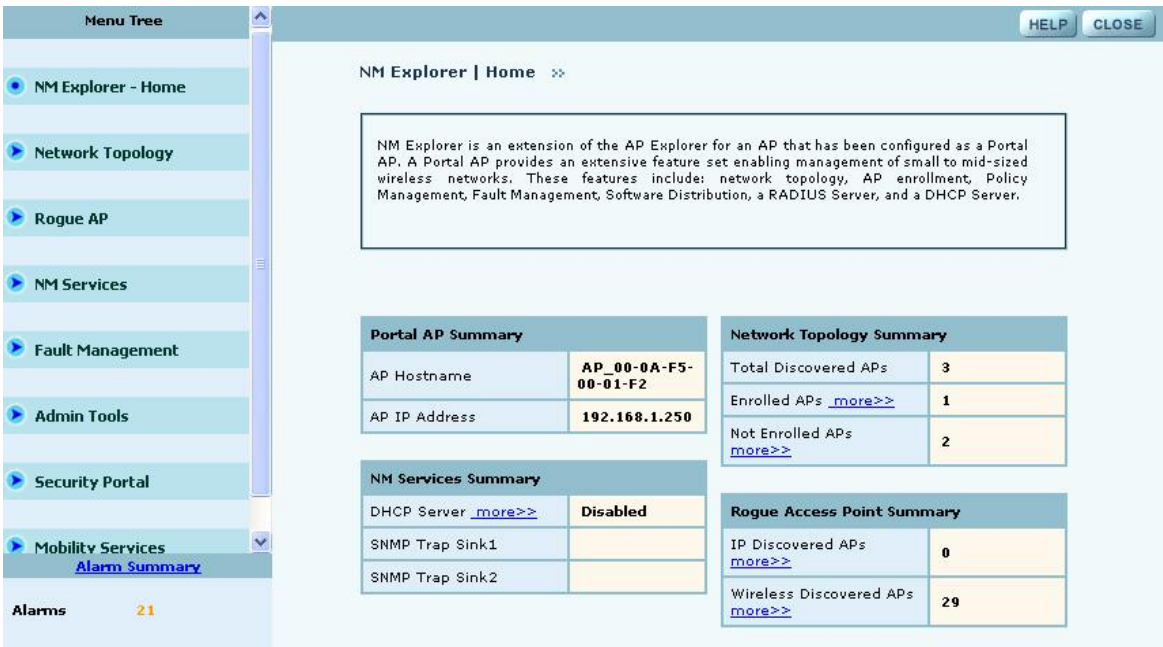
Using NM Portal

To use the Airgo AP for NM Portal services, it is necessary to initialize (bootstrap) the unit in NM Portal mode. Do so when initially configuring the AP, or by resetting the AP to factory defaults prior to booting. Chapter 3, “Installing the Access Point Using the Configuration Interfaces,” explains how to initialize an NM Portal and how to reset to factory defaults.

NOTE: Before resetting the AP to factory defaults, make sure to have the original password that was shipped with the unit available.

After the AP is initialized as a portal, access NM Portal services from the web interface at any time by clicking **Manage Wireless Network** on the menu tree or on the Home panel (“The Home Panel” on page 40). The NM Portal Network Management Explorer opens in a new browser window (Figure 127).

Figure 127: NM Portal Web Interface



This interface is similar to that of the standard Airgo AP web interface. The menu tree on the left contains a set of menus that provide access to application features. Use the detail panels on the right to set the configuration and monitor the state of the network. The alarm panel in the lower left portion of the window shows the number of outstanding critical alarms collected across the network managed by NM Portal.

Home Panel

The Home panel (Figure 127) contains summary information about the network configuration together with links to some of the Detail panels. Open the Home panel at any time by selecting **Home** from the menu tree.

Menu Tree

The menu tree contains the following menus:

- Home — Open the Home panel.
- Network Topology — Manage AP enrollment, wireless backhaul, IP address status, radio neighbors, and network inventory.
- Rogue AP — Classify and manage rogue APs.
- NM Services — Set up policies, network discovery, DHCP settings, and portal settings.
- Fault Management — View alarm logs and syslog events.
- Admin Tools — Upgrade AP software (see “Upgrading Software” on page 251).
- Security Portal — Add network, administrative, and legacy users, and enable the RADIUS proxy feature.
- Mobility Services — Configure and manage Layer-3 mobility services.

Each of these topics is described in this chapter, except Software Upgrade, which is described in Chapter 10, “Maintaining the Access Point.”

Click the arrow to the left of a menu item to expand the menu.

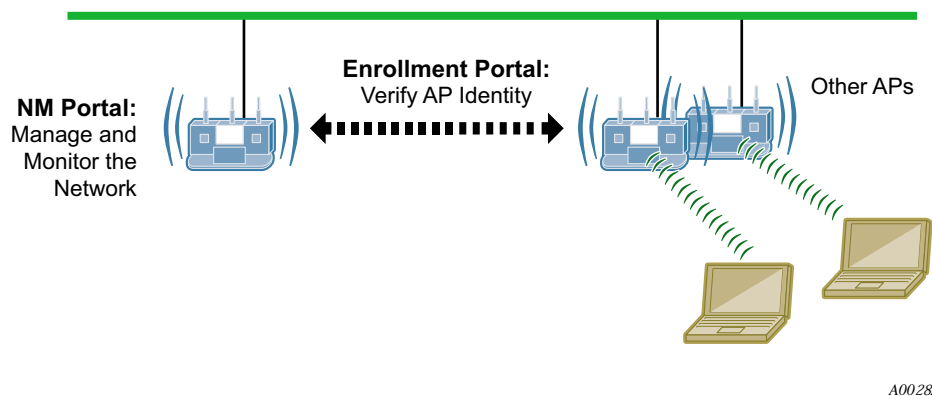
Using the Network Topology Menu

Use the Network Topology menu items to manage the identification, network status, and relationship of APs in the network.

Enrolling APs

Network security depends upon mutual trust between the NM Portal and the other managed Airgo APs. Each access point must trust the identity of the NM Portal AP, and the NM Portal must trust that each access point is fully authenticated (Figure 128).

Figure 128: AP Enrollment



Enrollment is the process used to establish this mutual trust. The process consists of several steps:

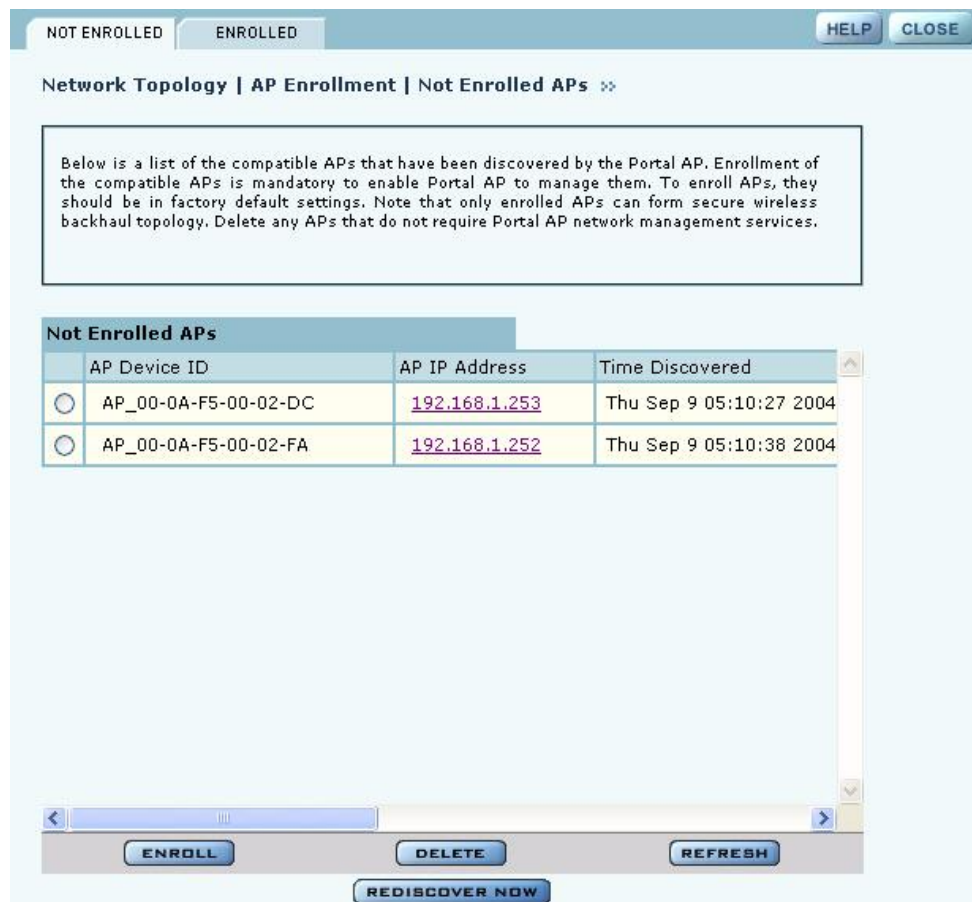
- NM Portal automatically discovers all the Airgo Access Points and presents those not already enrolled in a list of unenrolled APs.
- You select a candidate AP to enroll and verify its identity.
- NM Portal and the AP perform a mutual authentication process.

- Once the authentication is complete, the AP is enrolled. It is not necessary to enroll the AP again, even if power is lost to the unit.

NOTE: In order to enroll an AP, it must be in the factory default state. This assures that enrollment will be based on a known configuration.

An NM Portal can discover up to 50 APs across up to five subnets, and can enroll and manage up to 20 APs. To access the enrollment panel, choose **AP Enrollment** from the Network Topology menu. The AP Enrollment panel opens to display the list of discovered, but as yet un-enrolled, APs (see Figure 129).

Figure 129: Network Topology - AP Enrollment - Not Enrolled



Perform the following functions from this panel:

Function	Description
Enroll an AP	1 Select the desired AP, and click Enroll to open the Enroll an AP Entry panel (Figure 130). If the AP is not in the factory default state, a message is presented. Click the AP link to open the web interface for the AP and reset it to the factory default configuration. 2 After verifying the information on the panel (Table 15), enter the correct password, and click Enroll. It takes a couple of minutes to enroll the AP.
Delete an AP	Select an AP and click Delete to remove it from the list.

Function	Description
Refresh	Click to update the display.
Rediscover Now	Scan the network to discover APs and update the Not Enrolled APs table.

Figure 130: Network Topology - AP Enrollment - Enroll an AP Entry Panel

Enroll an AP

AP Device ID	AP_00-0A-F5-00-02-FA
IP Address	192.168.1.252
Serial Number	XXX00000762
Verify AP ThumbPrint	9f:ec:af:8e:2f:71:5a:60:54:6e:a0:32:79:dd:b2:13:26:0a:2b:18
AP Password *	
Confirm Password *	
Enable Security Portal	☐

ENROLL

CANCEL

The Enroll an AP panel contains information that uniquely identifies the AP. To verify the identity of the AP, compare the following information to the information on the paperwork shipped with the AP:

Table 15: AP Enrollment Information

Field	Description
AP Device ID	Verify the alphanumeric name of the AP. The default is the IP address.
IP Address	Verify the IP address of the AP.
Serial Number	Verify the AP serial number.
Thumbprint	Verify the thumbprint, which uniquely identifies the AP for security purposes.
Password	Enter and confirm the company-supplied password.
Security Portal	Indicate whether to use the AP as a standby security portal. With a backup security portal, a copy of the user authentication database remains accessible even if the NM Portal AP becomes unavailable.

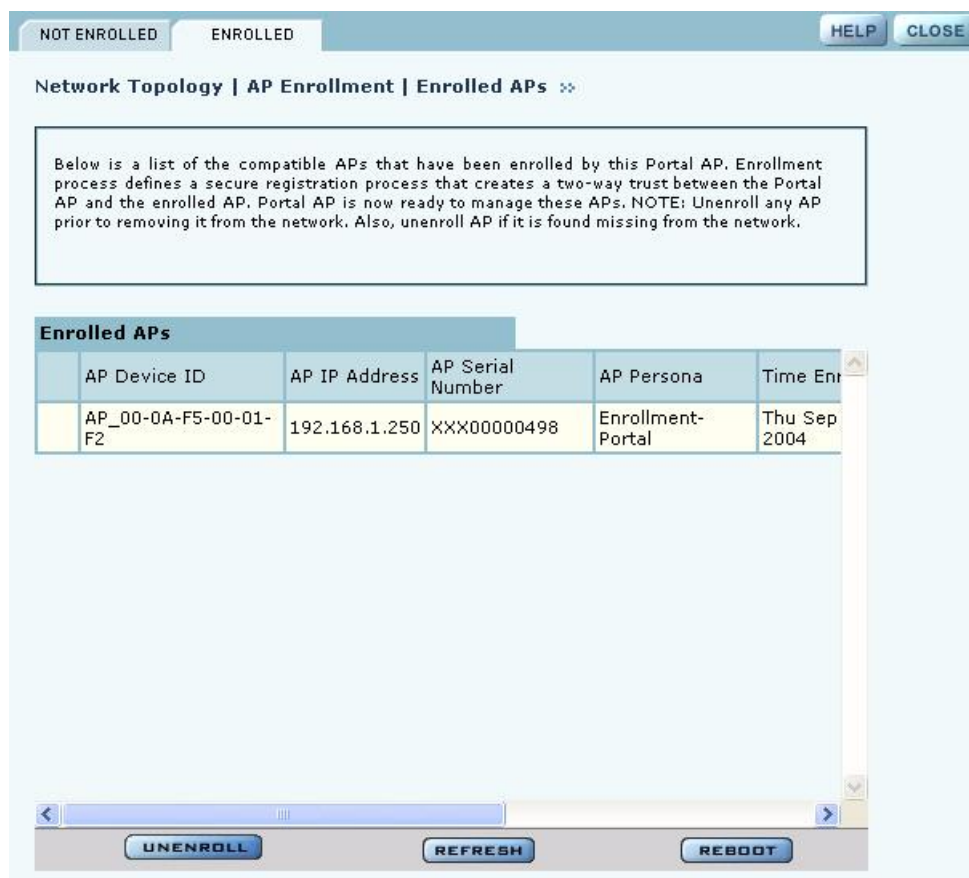
When an AP is enrolled, it is configured with the enrolling AP’s bootstrap configuration. Refer to Chapter 3, “Installing the Access Point Using the Configuration Interfaces,” for bootstrap configuration details.

Enrolled APs

Enrolled APs are listed on the Enrolled tab of the Enrollment panel (Figure 131). The screen should refresh automatically to reflect new enrollments. If this does not happen, click **Refresh**.



NOTE: If DHCP is used for address assignment for enrolled Airgo APs, the AP address may change periodically. When that occurs, service is not interrupted, and all security credentials remain intact.

Figure 131: Network Topology - AP Enrollment - Enrolled

Perform the following functions as needed from the Enrolled APs tab:

Function	Description
Unenroll	Remove the AP from the set of enrolled APs.
Refresh	Update the screen display to reflect the most recent enrollment changes.
Reboot	Reboot the selected AP.
Click the IP address link for an AP	Access the web interface for the selected AP in a new browser window.

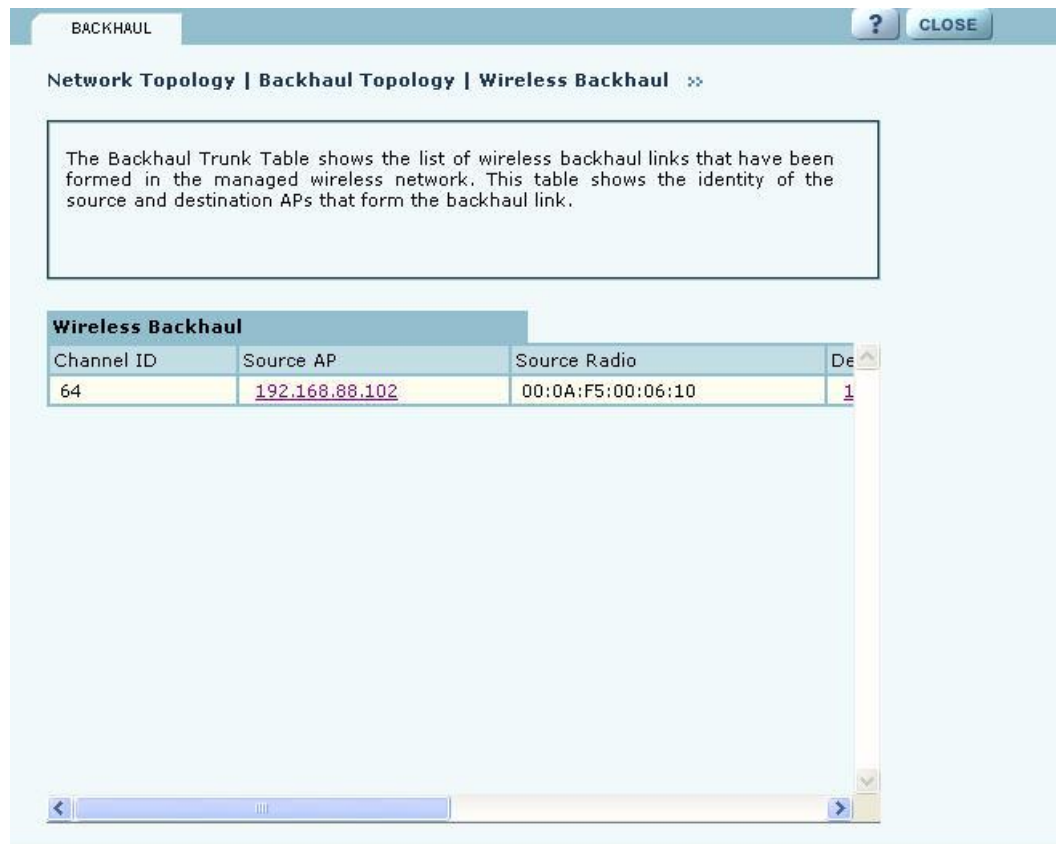
NOTE: When an AP is unenrolled, the mutual trust between the NM Portal and the AP is destroyed and the unenrolled AP resets to factory defaults. The AP cannot be configured by NM Portal nor participate in the network (i.e., form a wireless backhaul) without being enrolled again.

Viewing Backhaul Topology

Configuring a wireless backhaul extends wireless network coverage while reducing the number of APs that must be connected to the wired network. Chapter 6, “Configuring a Wireless Backhaul,” explains how to configure the Airgo AP to be part of a wireless backhaul. Once the wireless backhaul structure is in place, use the Backhaul Topology panel in NM Portal to view all the

backhaul paths defined for the network. Choose **Backhaul Topology** from the Network Topology menu to display this information (Figure 132).

Figure 132: Network Topology - Backhaul Topology



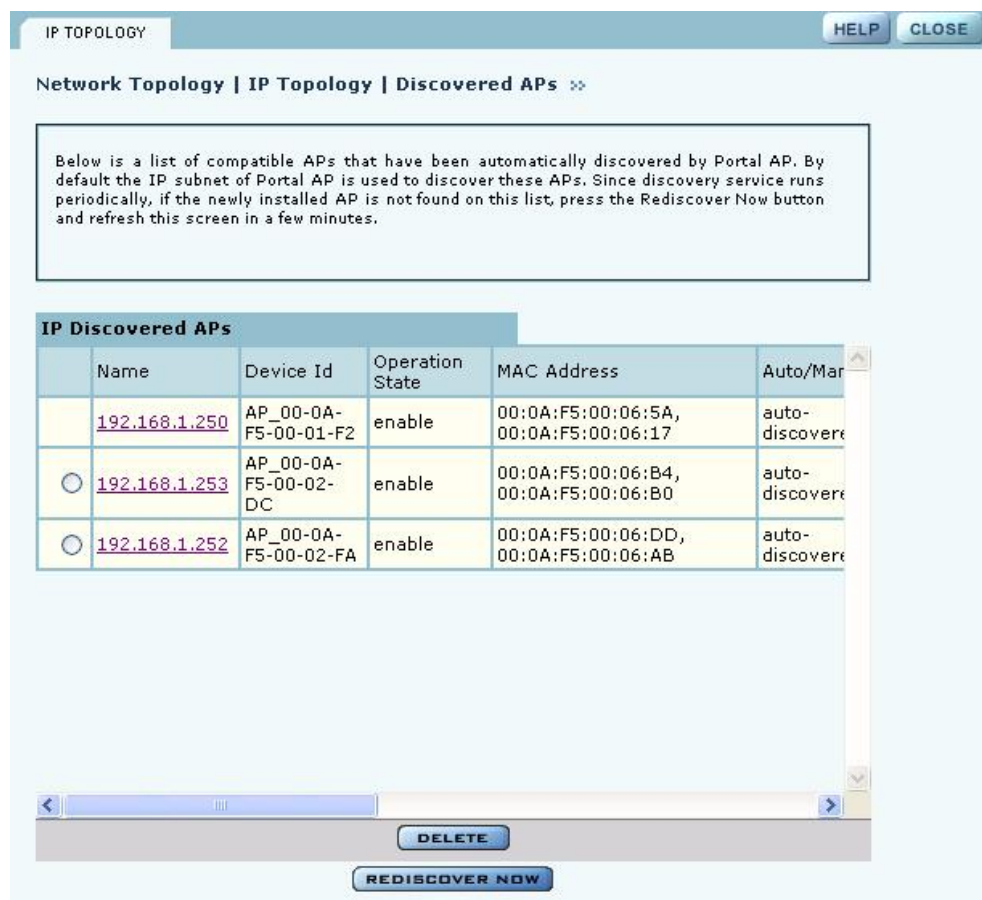
This panel contains the following information for each backhaul link:

Field	Description
Channel ID	RF channel over which the backhaul traffic travels.
Source AP	AP that begins the backhaul trunk. The Source AP link opens the web interface for the AP in a new browser window
Source Radio	MAC address of the radio used for the uplink (wlan0 or wlan1)
Destination AP	IP address of the AP that terminates the backhaul trunk.
Destination Radio	MAC address of the radio (could be wlan0 or wlan1) that ends the backhaul trunk
Retrunk Count	The number of times a functioning backhaul radio reestablishes a trunk (a new backhaul can be established to any AP within RF range, as retrunk does not necessarily mean re-connection to the same AP; if the retrunk count is high, the network has a high level of instability in its wireless inter-access point connections)
Rediscover Now button	Button that initiates the rediscovery process

Viewing IP Topology

The IP Topology panel lists all the APs discovered by NM Portal and the APs that were manually added to the network topology (see “Configuring Network Discovery” on page 200). Choose **IP Topology** from the Network Topology menu to display this information (Figure 133).

Figure 133: Network Topology - IP Topology



The table includes the following information for each AP:

Field	Description
Name	IP address assigned to the AP
Device ID	Unique AP identifier sent during the discovery process and required for AP enrollment (The device ID is included in the paperwork shipped with the AP.)
Operation State	Indication of whether the AP can be reached from the NM Portal AP (The operation state is updated once every five minutes.)
MAC Address	MAC addresses assigned to each of the AP radios (The address of the wlan0 radio is listed first and the wlan1 radio is listed second.)
Auto/Manual	Indication of whether the AP was discovered automatically or manually identified

Field	Description
Portal Services	Indication of which portal services are configured on the AP (enrollment and security). Possible values include: • Factory Default - AP has not yet been enrolled or bootstrapped. • Access Point - AP has been enrolled/bootstrapped as an AP. • NM Portal - AP is enrolled/bootstrapped as NM Portal. • SEC Portal - AP is enrolled/bootstrapped as a Security Portal. • NM & SEC Portal - AP is enrolled/bootstrapped as NM Portal and security portal. • Enrollment Portal - AP is bootstrapped as an enrollment portal.
Time Discovered	Date and time of discovery
Enrollment State	Indication of whether the AP is enrolled (authorized) or not (unauthorized)
Thumbprint	Unique identifier used for security purposes (The thumbprint is included in the paperwork shipped with the AP.)

View and check the status of all discovered APs from this panel. To delete an AP from the list, select the radio button to the left of the listing, and click **Delete**. Deleting an AP removes it from the topology database and deletes all the details about its configuration. However, because network discovery is a continuous process, it is possible for a deleted AP to be rediscovered if it is still part of the network.

Use the Delete feature when an AP is moved out of the network managed by this NM Portal, so that the portal no longer needs to track the AP. An enrolled AP must be unenrolled first before deleting it from the topology.

Displaying Discovered Radios

Every 15 minutes, the NM Portal AP polls all the enrolled APs, which then report on all the wireless devices they can detect. The results of the polling are presented in the Discovered Radio table (Figure 134), accessible from the Discovered Radios item under the Network Topology menu in the menu tree.

Use the Discovered Radios list to characterize the wireless network neighborhood and detect possible rogue APs.

Figure 134: Network Topology - Discovered Radios

Below is a list of AP radios detected by all enrolled APs in this network and reported to the Portal AP. These radios are discovered by wireless scanning and comprise both the authorized radios and the rogue candidates. Time Reported is the time at which this list was generated, while Time Discovered is the time at which the radio was first discovered.

Radio MAC Addr	IP Address	Reporting AP	Time Reported	Time Discovered
02:61:19:00:00:00			12:57:56	11:12:4
00:0A:F5:00:06:B0			12:57:56	11:57:4
00:09:5B:66:29:9E		AP_00-0A-F5-00-01-F2	12:57:56	12:57:4
00:0A:F5:00:06:B4			12:57:56	11:57:4
00:0A:F5:00:06:DC			12:57:56	11:57:4
00:0A:F5:00:06:FA			12:57:56	11:57:4
00:0A:F5:00:04:84			12:57:56	11:57:4

The Discovered Radios table contains the following information for each detected device:

Field	Description
MAC Address	Address that uniquely identifies the detected device.
IP Address	IP address of the detected device, if known.
Reporting AP	The enrolled AP that reported the device to the NM Portal AP. If this field is blank, the AP was reported on a previous scan but not the most recent one.
Time Reported	The time of the last scan that detected the AP.
Time Discovered	The time of day that the presence of the device was discovered by the reporting AP.
Class	Indication of whether the discovered node is just a Radio Neighbor or a Radio and IP Neighbor. Radio and IP neighbors are part of the internal network and are reachable by way of IP addressing.
Signal Strength	Strength of the detected signal in dBm.
SSID	The SSID of the detected device, if known.
Channel ID	The channel on which the signal was detected.
BSS Type	Whether the detected device is part of an infrastructure or ad-hoc service set.

Displaying Network Inventory

It is recommended that you run the same software and hardware versions on all the APs in the network. The Inventory Table panel provides a display of hardware and software version information for selected APs and can be used to monitor the consistency of configurations across the network.

To open the Inventory Table panel (Figure 135), select Network Inventory from the Network Topology menu.

Figure 135: Network Topology - Inventory Table

INVENTORY TABLE

HELP

CL

Network Topology | Network Inventory | Inventory Table

This page shows the inventory of APs in the network. It also shows the version of the H/W and S/W installed on these APs. It is recommended that all nodes in the network run the same version of the AP image.

Select the AP(s) for version details

☒ Version Details for Enrolled APs

☐ Version Details for AP

☐ Version Details for all discovered APs :

APPLY

RESET

AP Version Details

AP	Device ID	HW Version	System Board Version	Software Version	Software Build Number
192.168.89.19	AP_00-0A-F5-00-01-7D	1	1.0	1.2.0	139-l3mob
192.168.74.253	AP_00-0A-F5-00-02-1F	1	1.0	1.2.0	139-l3mob
192.168.74.242	AP_00-0A-F5-00-02-43	1	1.0	1.2.0	139-l3mob
192.168.89.51	AP_00-0A-F5-00-0C-1F	1	1.0	1.2.0	139-l3mob

REFRESH

Select one of the following sets of APs, and click Apply to display the version information. Click Reset to return to the previously saved value.

Option	Description
Version Details for Enrolled APs	Version information for APs that are enrolled
Version Details for AP	Version information for the AP with the entered IP address
Version Details for all discovered APs	Version information for all APs discovered by NM Portal

The AP Version table contains the following information for each AP:

Field	Description
AP	IP address of the AP
Device ID	Unique AP identifier sent during the discovery process and required for AP enrollment
HW Version	Release of hardware used in the AP
System Board Version	Release of system board hardware used in the AP
Software Version	Release of software used in the AP
Software Build Number	Sequence number indicating the exact software build used in the AP
Software Build Date	Date that the software was compiled
Software Licenses	Software licenses that are currently active on the AP

Managing Rogue Access Points

A rogue AP is an access point that connects to the wireless network without authorization. In some cases, the AP may be performing a legitimate function and the appropriate management action is to classify the AP as “known.” If it is not possible to identify a legitimate role for the AP, then the AP is considered to be a true rogue. NM Portal provides information to help determine where rogue APs are physically located and how recently they have accessed the network. With this information, it may be possible to find and disable them.

 **NOTE:** Use the Discovery Configuration panel to enable the rogue AP discovery feature. For instructions, see “Configuring Network Discovery” on page 200.

Potential rogue AP candidates are identified during discovery. Every 15 minutes, NM Portal scans the network to discover and identify known Airgo APs. The domain for the discovery process is specified in the Discovery Configuration panel (see “Configuring Network Discovery” on page 200). Discovery can be restricted to specific subnetworks, ranges of IP addresses, or individual APs. It is also possible to specify whether the discovery is at the IP (Layer-3) or wireless/MAC level (layer 2).

Wireless discovery is based on the beacon sent by APs within range of the receiving AP. Each AP collects information about beacons it sees and passes that information to NM Portal. NM Portal checks the MAC address of the detected AP to see whether it matches that of a known AP. If it does not match, the detected AP becomes a rogue AP candidate.

IP level discovery requires that the detecting AP be able to determine the IP address of the discovered AP through an IP / SNMP connectivity check and establish IP-level communications with it. NM Portal then performs a series of consistency checks and certification to determine whether the AP is a recognized part of the network.

After an AP is successfully discovered and authenticated, the system checks to see whether it is enrolled and places it into the Enrolled or APs to be Enrolled table. For more information on AP enrollment, see “Enrolling APs” on page 181. A variety of conditions may cause NM Portal to label an AP as a rogue candidate:

- The AP is not an Airgo AP.
- A problem exists with the AP certificate and the AP cannot be authenticated.
- The AP is a legitimate device on a neighboring network but has been detected through a wireless scan.
- An unauthorized device attempts to access the network

The objectives of rogue AP management are to determine which APs pose a security risk and to take action to reduce the risk.

The Rogue AP panels within NM Portal provide an interface to monitor and classify rogue APs. Use the IP Rogue AP panel to manage potential rogues detected through IP discovery, and use the Wireless Rogue AP panel to manage potential rogues detected through wireless discovery.

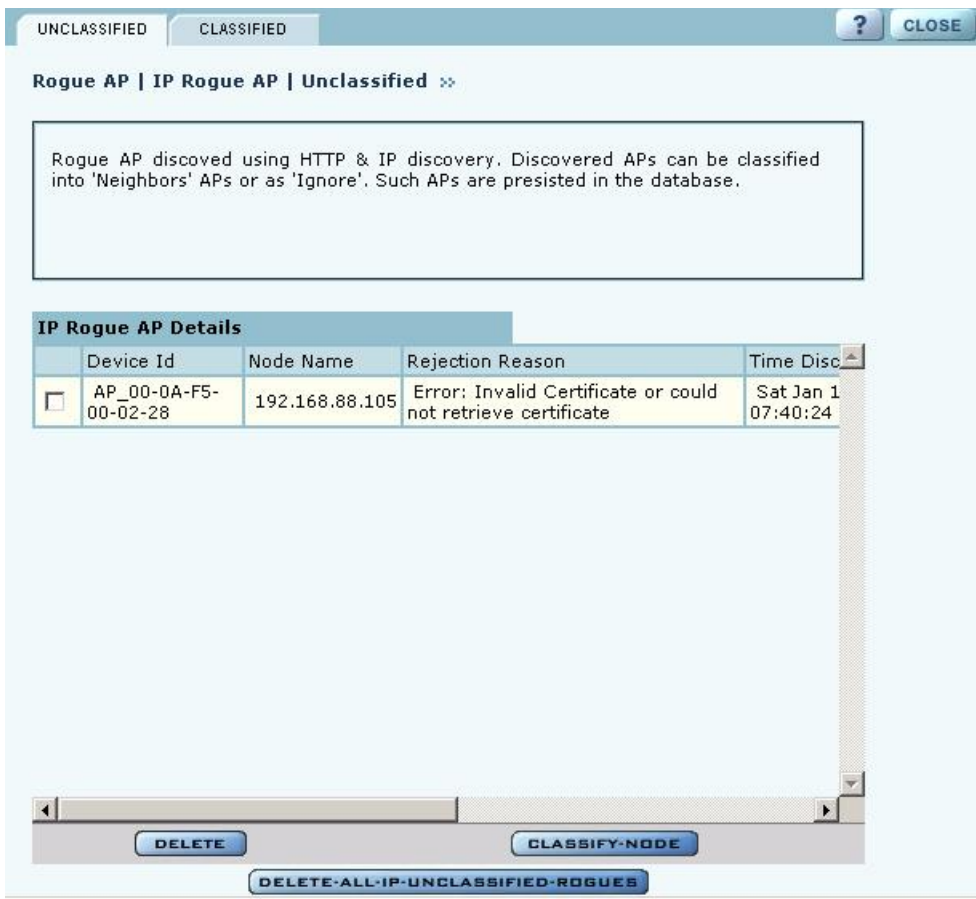
Each panel opens to the Unclassified tab, which lists the candidate rogue APs. From the list, select individual APs to classify as known in your network or a neighbor’s network. Once classified, the APs are listed in the IP or Wireless Classified tab.

IP Rogue AP Management

Select IP Rogue AP from the Rogue AP menu to open the table of IP-unclassified APs. This panel (Figure 136) lists the following information for each unclassified AP:

Field	Description
Device ID	Unique identifier for the AP
Node Name	Name of the AP advertised in the beacon frame
Rejection Reason	Failure that prevented the AP from passing authentication
Time Discovered	Time of the last IP scan that detected the AP, updated each time the AP is detected
Thumbprint	Factory-generated identifier used for AP enrollment

Figure 136: IP Rogue AP - Unclassified



Perform the following functions from this tab:

Function	Steps
Classify an AP as known	1 Select the AP from the list. APs are identified by device ID and IP address, if known. 2 Click Classify-Node to open the Classify the Rogue AP panel (Figure 137). 3 Select Our-Network to classify the AP as known within your wireless network. Select Neighbor-Network to classify the AP as known in a neighboring network. 4 Click Apply. The AP is now classified. The classification information is retained in the NM Portal database and presented on the Classified tab (Figure 138). This information is retained upon AP reboot.
Delete an AP from the rogue list	Click Delete and click OK to confirm. If an AP is deleted from the list and then discovered in a subsequent scan, it is added to the list again.
Delete from the list all APs classified as IP rogues	Click Delete all IP-Unclassified Rogues , and click OK to confirm.

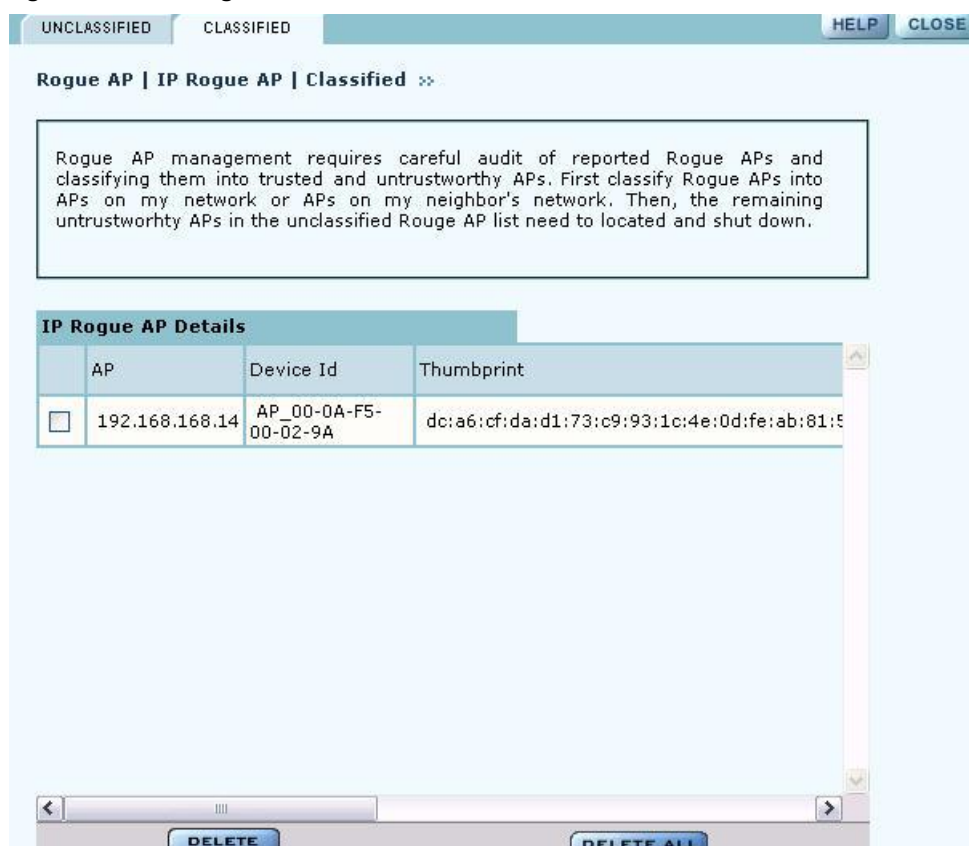
Figure 137: IP Rogue AP - Classify

Classify the Rogue AP	
Rogue AP IP Address	192.168.88.102
Rogue AP MAC Address	
Rogue AP Class	☒ Our-Network ☐ Neighbor-Network
APPLY RESET	

Classified Tab

The Classified tab (Figure 138) lists all the APs designated as known through IP classification. It contains the following information for each classified AP:

Field	Description
AP	Name of the AP, by default, the MAC address
Device ID	Unique identifier for the AP
Thumbprint	Factory-generated identifier used for AP enrollment
Portal Services	Portal services (enrollment, security, NM portal) configured on the AP
Operational State	Indicator of whether the AP is currently active
Discovery Method	IP or wireless discovery
Time Discovered	Time of the last IP scan that detected the AP (updated each time the AP is detected)
Node State	Identifies whether the AP has been classified as a member of Our-Network or Neighbor-Network
MAC Address	MAC address of the AP

Figure 138: IP Rogue AP - Classified

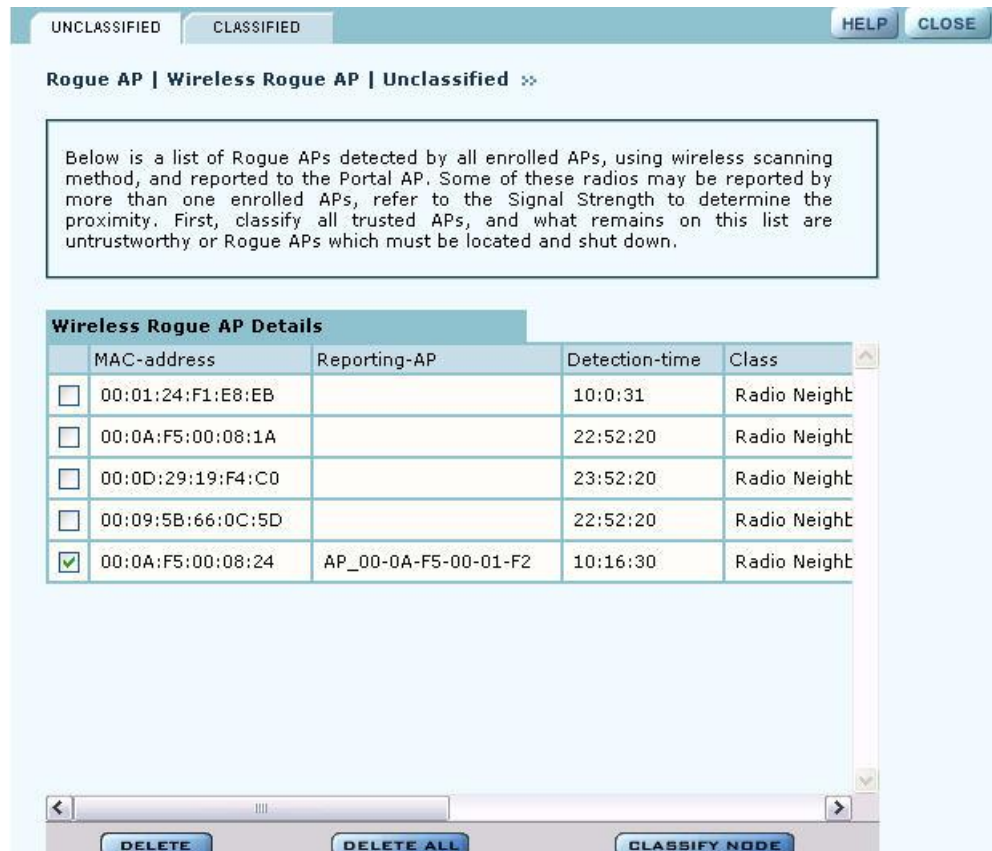
Wireless Rogue AP Management

Wireless rogue management differs from IP rogue management in the type of discovery used to determine whether the AP is authorized to be part of the network. In wireless discovery, each AP scans the beacons sent by other APs within range and attempts to identify the APs from the information in the beacon.

Select Wireless Rogue AP from the Rogue AP menu to open the table of unclassified wireless rogue APs. This panel (Figure 139) lists the following information for each IP rogue:

Field	Description
MAC Address	MAC address of the unclassified rogue AP
Reporting AP	The device ID of the AP or APs that identified the rogue AP (If this field is empty, the rogue device was detected in a previous scan, but not in the most recent scan.)
Detection Time	Time that the AP was last detected
Class	Radio Neighbor or Radio and IP Neighbor
Signal Strength	Strength of the beacon (dBm)
BSS Type	Infrastructure or ad-hoc (IBSS)
SSID	SSID sent in the rogue beacon
Channel ID	Radio channel on which the AP was discovered

Field	Description
Reporting Time	Time of the last wireless scan

Figure 139: Wireless Rogue AP - Unclassified

Perform the following functions from this tab:

Function	Steps
Classify an AP as known	1 Select the AP from the list. APs are identified by MAC address. 2 Click Classify-Node to open the Classify the Rogue AP panel (Figure 140). 3 Select Our-Network to classify the AP as known within your wireless network. Select Neighbor-Network to classify the AP as known in a neighboring network. 4 Click Apply. The AP is now classified. The classification information is retained in the NM Portal database and presented on the Classified tab (Figure 141). This information is retained upon AP reboot.
Delete an AP from the rogue list	Click Delete and click OK to confirm. If an AP is deleted from the list and then discovered in a subsequent scan, it is added to the list again.
Delete from the list all APs classified as wireless rogues	Click Delete All , and click OK to confirm.

Figure 140: Wireless Rogue AP - Classify

Classify the Rogue AP	
Rogue AP IP Address	
Rogue AP MAC Address	00:0A:F5:00:06:20
Rogue AP Class	☐ Our-Network ☒ Neighbor-Network
APPLY RESET	

Classified Tab

The Classified tab (Figure 141) lists all the APs designated as known through wireless classification. It contains the following information for each AP:

Field	Description
MAC Address	Name of the detected AP; by default, the MAC address
Reporting AP	Device ID of the AP that detected this rogue AP
Detection Time	Time of the scan that last detected the AP
Class	Category used to classify the AP

Figure 141: Wireless Rogue AP - Classified

UNCLASSIFIED CLASSIFIED HELP CLOSE

Rogue AP | Wireless Rogue AP | Classified »

Rogue AP management requires careful audit of reported Rogue APs and classifying them into trusted and untrustworthy APs. First classify Rogue APs into APs on my network or APs on my neighbor's network. Then, the remaining untrustworthy APs in the unclassified Rouge AP list need to located and shut down.

Wireless Rogue AP Details				
	MAC-address	Reporting-AP	Detection-time	Class
☐	00:0A:F5:00:08:24	AP_00-0A-F5-00-01-F2	10:16:30	Radio Neighbo

Using the NM Services Menu

Use the NM Services menu to define and manage policies, configure parameters for network discovery, add information about DHCP servers, and add portals at remote locations.

Working with Policies

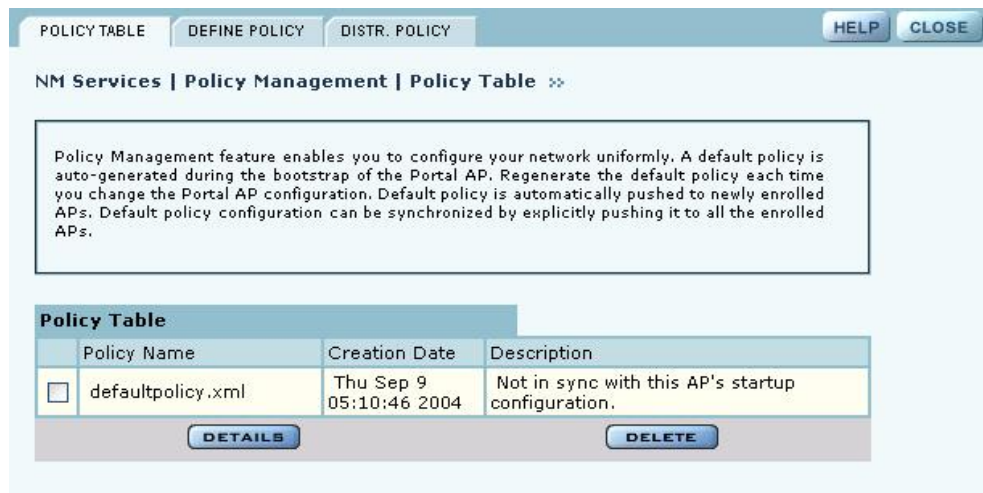
Policy Management provides tools to keep your network configuration synchronized to a defined set of rules. Open the Policy Management panel to manage configuration policies for distribution to the network of enrolled APs. The panel contains the following tabs:

- Policy Table — View existing policies.
- Define Policy — Specify a policy for bootstrapping other APs in the network.
- Distribute Policy — Send a policy to other APs in the network.

Policy Table

The policy table (Figure 142) lists policies that exist on this AP and are available for distribution to the network of enrolled APs.

Figure 142: NM Services - Policy Management - Policy Table



To view the details of a policy, select the name in the policy table, and click **Details**. The policy table expands to display all the parameters contained in the policy (Figure 143). To return to the policy table, click **Back**. To delete a policy, click **Delete**.

Figure 143: NM Services - Policy Management - Policy Table - Details (excerpt)

POLICY TABLE DEFINE POLICY DISTR. POLICY HELP CLOS

Display the content of current Policy. This shows all the configured attributes of this policy. Review carefully the configuration attributes prior to distributing this policy to the network.

Policy Details

Policy Name	defaultpolicy.xml	
config backhaul delete-uplink-bssid		
bssid		
config backhaul uplink-criteria		
interface	wlan0	
ssid	DeerCreekCo	
ipnetaddr	0.0.0.0/0	
path-selection	lowest-weighted-	
config backhaul uplink-criteria		
interface	wlan1	
ssid	DeerCreekCo	
ipnetaddr	0.0.0.0/0	
path-selection	lowest-weighted-	

< >

< BACK

Define Policy

Define a default policy for bootstrapping other APs in the network by selecting the configuration of this AP as a model. The default policy is pushed automatically to newly enrolled APs. Use the Define Policy tab (Figure 144) to choose the default policy.

NOTE: The NM Portal AP requires two radios in order to construct a default policy for two-radio APs.

Perform the following functions from this tab:

Function	Description
Generate a default policy from a pre-defined policy	Select a policy from the pull-down list, and click Apply . Not currently supported.
Use this AP's start-up configuration to generate a default policy.	Select the checkbox, and click Apply .

Figure 144: NM Services - Policy Management - Define Policy

The screenshot shows the 'Define Policy' tab selected. At the top are tabs for 'POLICY TABLE', 'DEFINE POLICY', and 'DISTR. POLICY', along with 'HELP' and 'CLOSE' buttons. Below the tabs is a breadcrumb trail: 'NM Services | Policy Management | Define Policy >>'. A text box contains instructions: 'Define a Default-Policy by selecting the configuration of this AP as a model for rest of the APs in the network. A Default-Policy is automatically pushed to newly enrolled APs. Note that Portal AP requires two radios in order to construct a default policy for 2-radio APs.' Below this is a section titled 'Generate Default Policy' with two rows: 'Use This Pre-defined Policy To Generate Default Policy' with a dropdown arrow, and 'Use This AP's Startup Config To Generate Default Policy' with a checked checkbox. A 'GENERATE DEFAULT POLICY' button is at the bottom.

Distribute Policy

Use the Distribute Policy tab (Figure 145) to direct how policies are shared across the network.

Figure 145: NM Services - Policy Management - Distribute Policy

The screenshot shows the 'Distribute Policy' tab selected. At the top are tabs for 'POLICY TABLE', 'DEFINE POLICY', and 'DISTR. POLICY', along with 'HELP' and 'CLOSE' buttons. Below the tabs is a breadcrumb trail: 'NM Services | Policy Management | Distribute Policy >>'. A text box contains instructions: 'Distribute a policy to one or more enrolled APs. Generally, default policy is the only policy that is recommended for distribution to the network, as it is derived from Portal AP's startup configuration. If other pre-defined policies are available, then when choosing Select All Policies To Distribute, ensure that none of these policies contain conflicting configuration options.' Below this is a section titled 'Distribute Policy' with two rows: 'Select Policy To Distribute' with a dropdown menu showing 'defaultpolicy.xml', and 'Select All Policies To Distribute' with an unchecked checkbox. Below these are four rows for selecting target APs, each with a checkbox and an IP address: 'Target AP Name', '192.168.88.101', '192.168.74.241', and '192.168.74.203'. A 'DISTRIBUTE NOW' button is at the bottom.

Configure the following fields on this tab:

Field	Description
Select Policy to Distribute	Select an existing policy from the pull-down list.
Select All Policies to Distribute	Select to distribute all the existing policies.

Field	Description
Target AP Name	Select the APs to receive the policy or policies, or select Target AP Name to distribute to all the APs.

Click **Distribute Now** to send the policies to the designated APs.

Configuring Network Discovery

Use the Network Discovery panel to set up the rules for AP discovery. The panel contains the following tabs:

- Configuration — Specify discovery parameters.
- Scope/Seed — Restrict discovery to specified subnetworks or IP address ranges.
- Rogue AP — Enable or disable rogue AP discovery.

Configuration

Select Network Discovery from the NM Services menu to open the Configuration panel (Figure 146).

Figure 146: NM Services - Discovery Configuration

CONFIGURATION SCOPE/SEED ROGUE AP HELP CLOSE

NM Services | Discovery Configuration | Configuration »

Portal AP support periodic IP discovery of compatible APs. It can discovery compatible APs across multiple IP subnets, but discovery is accelerated when it is seeded with the IP address of one of the compatible APs in each IP subnet. Since discovery service is run periodically, press the Rediscover Now button for immediate IP discovery initiation.

Discovery Interval and Limit Configuration

Discovery Interval (Minutes)

Discovery Limit

APPLY RESET

Manually Add an AP to Topology DB

AP IP Address

APPLY RESET

Start Discovery

Discovery Methods ☒ All ☐ IP ☐ Wireless

Force Rediscovery ☒

REDISCOVER NOW

Configure the following values on this tab:

Field	Description
Discovery Interval	Restrict discovery to a time interval (in minutes). The range is 60-10080 (default is 60 minutes). NOTE: Based on the default discovery interval, a newly installed AP could take one to two hours to be discovered. Use Force Rediscovery to speed the process.
Discovery Limit	Restrict discovery to a number of APs. Once this limit is reached, the discovery process stops. The range is 1-50 (default is 50 APs).
AP IP Address	Specify the IP address of an AP that you want to manage but which is not part of the managed subnetwork specified in the discovery scope. APs added to the managed network this way are termed “manually added” and can be managed by NM Portal. This option is useful if you want to manage just a few APs in a different subnet without incurring the overhead associated with discovering all the APs in that subnet. If an enrolled AP is moved to a different subnet not managed by the NM Portal, then the Portal will automatically flag that AP as a manually added AP and will continue to manage that AP.
Discovery Methods	Select whether to discover the APs with valid IP address information (IP), or those identifiable by their radio beacon (Wireless), or those that meet either criterion.
Force Rediscovery	Select to force an immediate rediscovery of all APs. If the discovery process is already in progress when rediscovery is initiated, then no additional discovery is re-initiated. To stop the current discovery process and restart discovery again, use the Force All option. This is useful if the discovery scope is incorrectly configured and must be deleted.

Click **Apply** to implement the changes in each section or **Reset** to return to previously saved values.

Use the Start Discovery radio buttons at the bottom of the panel to configure discovery on demand. Choices are to discover all APs, only those with a connection to the wired network (IP), or only those that radio neighbors. Click **Rediscover Now** to rediscover the network on demand.

Scope/Seed

By default, NM Portal automatically discovers all compatible APs in the local IP subnet. When APs are deployed across multiple subnetworks, specifying the discovery scope and seed IP address speeds the discovery process. The seed IP address is used as the reference AP for discovery purposes. The Seed AP is optional. If it is not specified, NM Portal automatically discovers all the compatible APs in that subnet and identifies a seed AP for itself.

Select the Scope/Seed tab (Figure 146) to configure the scope and seed parameters.

Figure 147: NM Services - Discovery Configuration - Scope/Seed

Portal AP support periodic IP discovery of compatible APs. It can discovery compatible APs across multiple IP subnets, but discovery is accelerated when it is seeded with the IP address of one of the compatible APs in each IP subnet. Since discovery service is run periodically, press the Rediscover Now button for immediate IP discovery initiation.

Discovery Scope and Seed Configuration

Discovery Scope - IP Network Address

Discovery Scope - Subnet Maskbits

Discovery Seed - AP IP Address

APPLY **RESET**

Discovery Scope Table

☐	Discovery Scope IP Subnet	Discovery Seed AP IP Address
☐	192.168.92.1/24	192.168.92.56
☐	192.168.74.1/23	192.168.74.253
☐	192.168.88.1/24	192.168.88.125
☐	192.168.89.1/24	192.168.89.51

DELETE

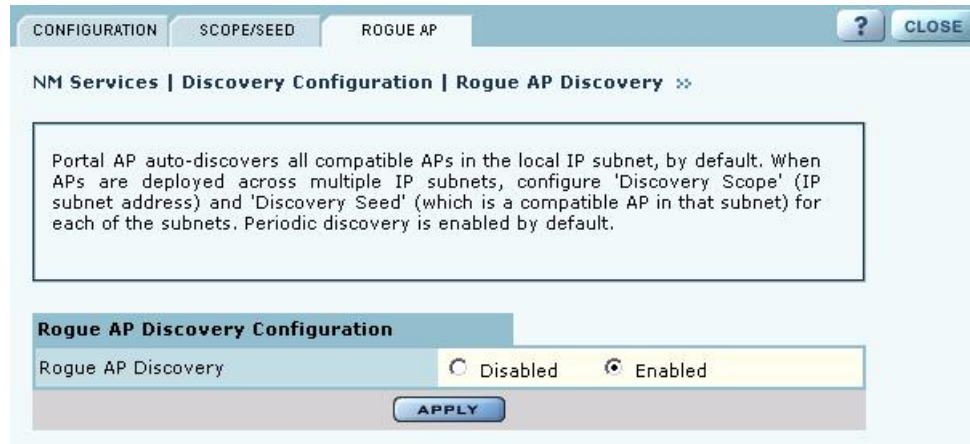
Configure the following fields on this tab:

Field	Description
Discovery Scope - IP Network Address	Enter the IP address of the subnet that you want to discover.
Discovery Scope - Subnet Maskbits	Enter the subnet prefix length for the discovery scope.
Discovery Seed	Specify a seed IP, which is the first address NM Portal will attempt to discover in the selected subnetwork.

Click **Apply** to save the selections and add them to the Discovery Scope Table at the bottom of the panel. To delete an entry from the Discovery Scope table, select the entry and click **Delete**.

Rogue AP

Use the Rogue AP tab (Figure 146) to enable or disable discovery of rogue access points. The default is Enabled. Click **Apply** to save the setting. If enabled, NM Portal automatically scans the network to detect IP and wireless rogue access points. For more information, see “Managing Rogue Access Points” on page 190.

Figure 148: NM Services - Discovery Configuration - Rogue AP

Configuring Portals

The Portal Configuration panel lists all the Airgo Access Point portals that your AP has discovered and permits addition of a standby security portal to ensure that the wireless user authentication service remains available even if the NM Portal AP temporarily loses its connection. The panel contains two tabs:

- Portal Table — Add a redundant security portal and synchronize the portal databases.
- Secure Backup — Use https to perform a secure backup of the NM Portal AP configuration.
- Portal Backup — Back up or restore the portal databases and configuration.

Portal Table

Use the Portal Table (Figure 149) to manage the security portals for the network.

Figure 149: NM Services - Portal Configuration - Portal Table

PORTAL TABLE | SECURE BACKUP | PORTAL BACKUP | HELP | CLOSE

NM Services | Portal Configuration | Portal Table »

The Portal Table lists the current set of portal APs. A single AP can provide all management services (enrollment, NM and security). An additional AP can provide redundant security service by mirroring the RADIUS database of the portal AP so that continuous authentication service can be provided to wireless users when the primary portal AP is undergoing maintenance.

Add Redundant Security Portal

AP IP-Address

Portal Table

AP	AP Device-Id	Enrollment Status
192.168.168.24	AP_00-0A-F5-00-01-F2	Enrolled
☐ 192.168.168.21	AP_00-0A-F5-00-02-E2	Unenrolled

Auto-Synchronize Databases

Sync Frequency (minutes) ☐ Default ☐ Periodic

DB Version Table

AP IP Address	Radius Client DB Version	Radius User DB Version	Certificate DB Version	AP Device-ID	Enrollment Status
192.168.168.24	1.0	1.0	1.0	AP_00-0A-F5-00-01-F2	Enrolled

Perform the following functions on this tab:

Field	Description
Add Redundant Security Portal	Specify the IP address, and click Apply . Only an already-enrolled AP can be configured to be a redundant security portal.
Portal Table	View the list of currently identified NM Portal APs. The listing includes the IP address of the AP, its device ID, and whether the AP is currently enrolled. To delete an entry from the table, select the radio button to the left of the entry, and click Delete . NOTE: All Portals shown in this table as unenrolled are currently not managed by this NM Portal but form part of other managed networks. Only Portals managed by this NM Portal will be shown as Enrolled and or will have a radio button that deletes the portal.

Field	Description
Sync Frequency	Select to automatically synchronize the database between the portals. The sync frequency represents the duration in minutes at which NM Portal cross checks the portals in the network to make sure their databases are synchronized with the NM Portal database. Click Apply to save the settings, or click Reset to return to the default values (autonomous selected, period five minutes). It is recommended that you accept the default value to make sure that synchronization takes place.
Portal DB Version Table	View current database information for user security. For each enrolled AP, the table lists the following information: • AP IP Address — IP address of each portal AP • RADIUS Client DB Version — Version of the user database resident on the RADIUS client • RADIUS User DB Version — Version of the user database for RADIUS users • Certificate DB Version — Version of the security certificate for RADIUS clients • AP Device-ID — Unique identifier for the AP • Enrollment Status — Indication of whether the AP is enrolled

Secure Backup

Use the Secure Backup tab (Figure 149) to save the NM Portal database and configuration using the secure https protocol.

Figure 150: NM Services - Portal Configuration - Secure Backup

PORTAL TABLE SECURE BACKUP PORTAL BACKUP HELP CLOSE

NM Services | Portal Configuration | Secure Backup »

Portal AP should be periodically backed up and would contain all portal databases and configuration. It is recommended to mirror Security Portal to avoid disruption while Portal AP is down. NOTE: Before restoring backed up portal database to a brand new AP, ensure that the new AP retains the same IP address as this portal AP.

Backup Portal Configuration

Save Current Configuration **SAVE CONFIGURATION**

Click Link to Download Configuration

Restore Portal Configuration

From file **Browse...**

APPLY **RESET**

Click **Save Configuration**. When the configuration is generated, a hyperlink is displayed. Right-click and select **Save As** to save the configuration locally. After the configuration file is saved, click **Delete** to remove the file from the AP. The file takes up space in AP persistent storage, so it is recommended that you remove it. To restore the configuration, browse to select the file, and then click **Apply** to restore the configuration and reboot the AP.

Portal Backup

Use the Portal Backup tab (Figure 151) to back up the portal databases and configuration to a TFTP server and to restore the configuration from the TFTP server. To back up and restore, enter the server IP address and specify a backup file name. To restore, enter the same TFTP server address and file name. If you want to reboot the AP once the configuration file has been copied, select **Reboot**. (required)

Figure 151: NM Services - Portal Configuration - Backup/Restore

PORTAL TABLE SECURE BACKUP **PORTAL BACKUP** HELP CLOSE

NM Services | Portal Configuration | Portal Backup »

Portal AP should be periodically backed up and would contain all portal databases and configuration. It is recommended to mirror Security Portal to avoid disruption while Portal AP is down. NOTE: Before restoring backed up portal database to a brand new AP, ensure that the new AP retains the same IP address as this portal AP.

Backup Portal Databases and Configuration

TFTP Server * 192.168.168.1

To File AP4_021004

APPLY RESET

Restore Portal Databases and Configuration

TFTP Server *

From File *

Reboot ☒

APPLY RESET

Configuring the DHCP Server

NM Portal includes an internal DHCP server, which can be activated to support IP address assignments in the network if a DHCP server is not in place. Choose **DHCP** from the NM Services menu to open the DHCP panel. The panel contains the following tabs:

- DHCP Options — Activate and configure the DHCP server.
- IP Range — Enter address information for the DHCP server.
- Leases — View details about the current DHCP leases.
- Static IP — Assign static IP addresses for specific equipment.

i **NOTE:** Use the DHCP panels to support IP address assignments only if a DHCP server is not already in place on the existing network.

i **NOTE:** The DHCP server on the NM Portal AP is bound to the default VLAN (VLAN ID 1). It serves address requests only for this VLAN.

DHCP Options

Select the DHCP Options tab (Figure 152) to activate and configure the DHCP server.

Figure 152: NM Services - DHCP Configuration - DHCP Options

NM Services | DHCP Server | DHCP Options »

For small to mid-sized wireless networks, a DHCP Server is available as a Portal AP feature for IP address resolution. To insure centralized IP address management, an external DHCP server should be implemented. DHCP server options can be configured below.

DHCP Server Admin State

Enable DHCP Server ☐

APPLY

DHCP Options Configuration

Lease Time (Hours)	1
Max Leases	
Gateway IP Address	
Current DNS Server IP Address	
DNS Server IP Address	
Current WINS Server Address	
WINS Server Address	
Current NTP Server IP Address	
NTP Server IP Address	

ADD **RESET**

To activate the server, **Enable DHCP Server** and configure the following information:

Field	Description
Lease Time	Specify the maximum number of leases that the server should assign. This is used to restrict the number of IP addresses served even though the IP subnet served by the DHCP server may be large. The default is one hour.
Max Leases	Specify the maximum number of available leases. There is no default.
Gateway IP Address	Enter the IP address of the gateway. There is no default.
DNS Server IP Address	Enter the IP address of the server or servers that provide domain name resolution. There is no default. More than one DNS IP address may be specified (space separated). If the field is left blank, then any previously configured DNS server addresses will be deleted. If you delete DNS servers, only those added manually are deleted. DHCP-assigned DNS servers continue to be available.
WINS Server	Enter the IP address of the Windows name server used to map IP addresses to computer names. There is no default.

Field	Description
NTP Server	Enter the IP address of the server or servers used to synchronize network clocks. There is no default. More than one NTP IP address may be specified (space separated). If you delete NTP servers, only those added manually are deleted. DHCP-assigned NTP servers continue to be available.

Click **Add** to save the configuration information.

IP Range

Select **IP Range** to configure address ranges for DHCP leases (Figure 153).

Figure 153: NM Services - DHCP Configuration - IP Range

NM Services | DHCP Server | IP Address Range ✕

By default, the DHCP Server requests from client on all AP interfaces and is therefore bound to the default bridge (br1). The IP Address Range for DHCP client leases can be limited by an IP address/mask-bits or by an explicit IP subnet start and end IP address.

DHCP IP Address Range

IP Subnet/Maskbits ☐

Use Fixed IP Address Range ☒

Start IP Address

End IP Address

ADD **RESET**

DHCP IP Address Range Table

Interface	IP Address Range	Start IP	End IP
br1	192.168.1.0/24	192.168.1.5	192.168.1.253

DELETE

Enter the following information on this panel:

Field	Description
Interface Name	Confirm the alphanumeric name of the AP interface. The default is br1, which is the default bridge.
IP Address Range	Select a radio button to specify the range of addresses available for assignment. Choose either of the following: - IP Subnet/Maskbits — Enter the address and maskbits that define the subnet to be used for address assignment. - Use Fixed IP Address Range — Specify a range of IP addresses by entering starting and ending addresses, with subnet prefix length.

Click **Apply** to save the address information. Add additional interfaces if desired. The added interfaces are listed in the DHCP Address Range table at the bottom of the panel. To delete a DHCP interface, select the interface in the DHCP IP Address Range table, and click **Delete**.

Leases

The Leases tab (Figure 154) lists each network computer serviced by DHCP and its lease information.

Figure 154: NM Services - DHCP Configuration - Leases

The DHCP lease table shows the current list of IP address that have been leased out by the DHCP server running on this AP.

MAC Address	Leased IP Address	Lease Time Remaining
00:0a:f5:00:06:8b	192.168.1.132	0 days, 0 hours, 59 minutes, 33 seconds
00:0a:f5:00:05:fe	192.168.1.131	0 days, 0 hours, 59 minutes, 36 seconds

This table contains the following information:

Field	Description
MAC Address	Address that uniquely defines the DHCP client
Leased IP Address	IP address assigned by the DHCP server
Lease Time Remaining	Amount of time remaining on the current DHCP lease (in hours)

Static IP

Use the Static IP tab (Figure 155) to reserve static IP addresses for specific nodes.

Figure 155: NM Services - DHCP Configuration - Static IP

Assign a static IP address to node whose IP address should never expire. Specify FQDN (or Fully Qualified Domain Name); node's MAC address to pin the static IP address to; and the static IP address from the configured IP address range. The static IP address assignment table lists the currently assigned IP addresses.

Static IP Address Configuration

Client Fully Qualified Domain Name

Client MAC Address

Assigned IP Address/Maskbits

ADD **RESET**

DHCP Static IP Address Table

☐	Client FQDN	Client MAC Address	Assigned IP Address
DELETE			

Enter the following information on this tab:

Field	Description
Client Fully Qualified Domain Name	Enter an alphanumeric name for the node, which is fully qualified by DNS.
Client MAC Address	Enter the MAC address that uniquely identifies the client station.
Assigned IP Address/Maskbits	Assign the static IP address and maskbits.

Click **Add** to save the information. The new entry is listed in the table at the bottom of the tab. To delete an entry, select the name in the DHCP Static IP Table, and click **Delete**.

Managing Network Faults

NM Portal aggregates alarms from all managed APs. Each AP can store up to 260 alarms locally. When the number of alarms exceeds this limit, the oldest alarms are deleted as needed. Use the Fault Management panels to view the system alarms and syslog entries. Alarms are raised as SNMP Traps, which are forwarded to the SNMP Sink Host (or Primary NMS).

Viewing Alarms

Choose **Alarm Summary** from the Fault Management menu to view counts and descriptions of alarms that occur in the network managed by NM Portal.

The Alarm Summary panel contains three tabs:

- Alarm Summary — View counts of system alarms in the managed network.
- Alarm Table — View a detailed list of alarms.
- Filter Table — Select events that should be filtered out of the reported alarm list.

Alarm Summary

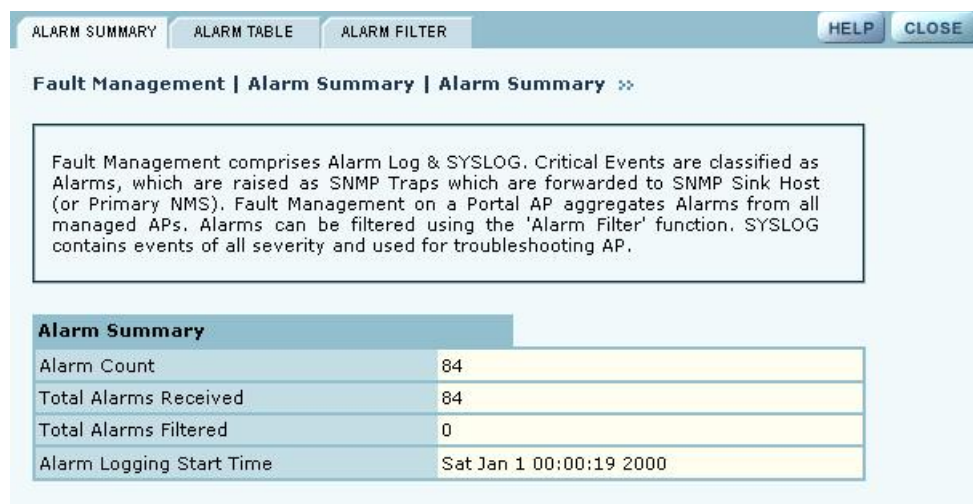
The Alarm Summary tab (Figure 156) provides an aggregate count of alarms across the network managed by NM Portal.

NOTE: The alarm count in the lower left corner of the Network Management Explorer window is the same as that given on the Alarm Summary tab. Click the Alarm Summary hyperlink to open the Alarm Summary tab.

The Alarm Summary tab contains the following information:

Field	Description
Alarm Count	Total alarms in the managed network
Total Alarms Received	Total alarms from APs other than this AP
Total Alarms Filtered	Count of alarms not displayed because they were filtered out
Alarm Logging Start Time	Time at which the counts began

Figure 156: Fault Management - Alarm Summary



Alarm Table

The Alarm Table tab (Figure 157) provides a detailed description of alarms and enables filtering of the alarm table for easy viewing and searching. A description of all the alarms is provided in “Airgo Access Point Alarms” on page 214 and additional details are presented in Appendix D, “Alarms.”

The Alarm Table includes the following information:

Field	Description
Alarm ID	Text description of the specific alarm

Field	Description
Alarm From	Device ID of the AP that reported the alarm
Description	Text description of the event
Log Time	Time the alarm occurred and was logged
From Module	The subsystem that is the source of the alarm. Modules include: • Authentication • Networking • Distribution • Configuration • Wireless • Discovery • NM Portal • SW Download

 **NOTE:** The filtering function on the Alarm Table tab only affects the information displayed in the Alarm Table at the bottom of the tab. To remove some event types completely from the alarm list, use the Alarm Filter tab.

Figure 157: Fault Management - Alarm Summary - Alarm Table

Alarm Summary | Alarm Table »

The Alarm Table lists all of the alarms logged by the selected AP. Alarms can be filtered based on the following criteria: Alarm ID, Logging Module ID, From AP, or Logging Time. Note: The Alarm Table is a finite-sized push-up stack where the oldest alarms roll off the top and the newest alarms are on the bottom.

Filter Configuration for Alarm Table

Alarm ID: BP authentication failed

Logging Module Name: Wireless (VWSM)

Alarms From (Host Address): AP_00-0A-F5-00-01-F2

Logging Period (mm/dd/yyyy): 02 / 09 / 2004 Date From

02 / 10 / 2004 Date To

SET FILTER **RESET**

Alarm Table (Filtered)

Alarm ID	Alarm From	Description
Management IP address changed	AP_00-0A-F5-00-01-F2	The management IP Address of node AP_00-0A-F5-00-01-F2 changed from 192.168.1.254 to NewIP 192.168.168.24
Radio enabled	AP_00-0A-F5-00-01-F2	Device ID AP_00-0A-F5-00-01-F2 radio 6 is en operating on 64
Radio enabled	AP_00-0A-F5-00-01-F2	Device ID AP_00-0A-F5-00-01-F2 radio 4 is en operating on 6

Configure the following fields to define a viewing filter:

Field	Description
Alarm ID	Select an alarm from the list to view only those specific alarms.
Logging Module Name	Select from the list to filter all the alarms from a specific system logging module.
Alarms From (Host Address)	Select an AP to view only the alarms generated by that AP.
Logging Period	Enter a date range to show events during a specific interval of time.

Click **Set Filter** to apply the filter to the alarm table or **Reset** to clear the selected values.

Table 16: Airgo Access Point Alarms

Alarm ID	Description
Discovered New Node	Generated when a new Airgo Access Point is discovered by NM Portal for the first time.
Node Deleted from Network	Generated when a previously-discovered node is deleted from the system. When the node is deleted, all information about that node is deleted from NM Portal. If the node's IP address falls within the discovery scope, then the node will be rediscovered and added back to the set of the discovered nodes during the next discovery scan.
Managed Nodes Limit Exceeded	Generated when the number of discovered nodes exceeds the limit defined in the Discovery Configuration panel, Configuration tab. See "Configuring Network Discovery" on page 200). If this alarm occurs, NM Portal ceases to discover or track any new nodes.
Node Enrolled	Generated when an Airgo AP has been successfully enrolled.
Node Un-Enrolled	Generated when an Airgo AP has been successfully rejected (un-enrolled).
Policy Download Successful	Generated when a policy is successfully downloaded to an AP.
Policy Download Failed	Generated when policy downloaded to an AP is unsuccessful due to an error in the policy, software version mismatch, or another error.
Image Download Succeeded.	Generated when an image is successfully downloaded and applied to an AP.
Image Download Failed	Generated when image download to an AP is unsuccessful, due to corrupted images, images of invalid length, or connectivity failures.
Software Distribution Succeed	Generated when an image distribution is completed.
Radio Enabled (BSS Enabled)	Generated when an AP radio is enabled. Indicates successful start of a BSS and includes the channel on which the AP radio will be operating.
Radio Disabled (BSS Disabled)	Generated when an AP is disabled. Disabling can be user triggered for administrative purposes, caused by radio reset due to application of wireless configuration parameters, triggered by hardware, or due to a change in SSID.
BSS Enabling Failed	Generated when an attempt to enable an AP radio fails. Reason codes: 0 – Unspecified reason 1 – System timeout attempting to enable BSS
Frequency Changed	Generated when operating frequency is changed for an AP radio due to user intervention or events such as periodic dynamic frequency selection (DFS). Reason Codes: 0 - Triggered due to DFS 1 - User triggered

Table 16: Airgo Access Point Alarms (continued)

Alarm ID	Description
STA Association Failed	Generated when an 802.11 client station fails in its attempt to associate to the AP radio. Reason Codes: 1 - Invalid parameters received from station in association request 2 - Only stations are allowed to associate with this AP based on current configuration 3 - Only backhauls can be formed with this AP based on current configuration 4 - Max backhaul limit is reached based on the 'Max Trunks' configuration for AP admission criteria 5 - Max station limit is reached based on the 'Max Stations' configuration for SSID 6 - SSID received in association request does not match SSID in AP configuration. This can occur more often when an AP is not broadcasting SSID in beacon (due to suppressed SSID or multiple SSIDs being configured) and station is associating to an AP with a different SSID 7 - Authentication and encryption requested by station does not match security policy of the AP 8 - Multi Vendor Station indicates that the station is not allowed to associate based on AP admission criteria 9 - 802.11b stations are not allowed to associate based on AP admission criteria 10 - Station is not allowed to associate and was transferred to another AP radio due to load balancing 11 - Station is not allowed to associate because node does not have network connectivity
STA Associated	Generated when a client station succeeds in associating to the AP radio. The alarm message includes the current associated stations, type of association, and user ID. The user ID is the user name if RADIUS authentication is employed; otherwise the MAC address is used.
STA Disassociated	Generated when an 802.11 station is disassociated by the network or the station. Reason Codes: 0 - Station initiated disassociation 1 - Station has handed off to another AP 2 - Disassociation triggered due to authentication failure after ULAP timeout 3 - Disassociation triggered due to user action

Table 16: Airgo Access Point Alarms (continued)

Alarm ID	Description
WDS Failed	Generated when wireless backhaul formation fails. The message includes the MAC address of the end node. This alarm can help track losses in network connectivity. Reason Codes: 0 - System failure 1 - Maximum BP count has been reached (this relevant only for AP) 2 - Join attempt to the uplink AP failed (BP side only)
WDS Up	Generated when a wireless backhaul formation succeeds. The message includes the MAC address of the end node. Reason Codes: 0 - Trunk has been established 1 - Trunk has been optimized (re-established based on better connectivity)
WDS Down	This is a notification generated when a wireless backhaul has gone down. The remote end's MAC address is provided. Reason Codes: 0 - System reason (unspecified) 1 - Loss of link (applies to BP side only) 2 - Trunk brought down by uplink AP (applies to BP side only) 3 - User retransmission issued (this can occur due to new backhaul configuration being applied on BP) 4 - Trunk has reformed with another AP (AP side only) 5 - Trunk brought down by BP (applies to AP side only)
Guest Authentication Succeeded	Generated when a guest station is authenticated and indicates the successful start of a guest access communications session. The guest user is offered the communications services specified in the guest profile for the specified SSID.
Guest Authentication Failed	Generated when a guest station fails to authenticate.
User Reject by RADIUS Server	Generated when user authentication fails. The AP radio and the RADIUS server that rejected the user are included in the message.
BP Rejected by RADIUS Server	Generated when a security portal has rejected the attempt by a BP radio to associate to the AP. This may mean that the BP is not enrolled in the same network as the AP or that the BP was just enrolled, but the enrollment database has not yet been synchronized across the network to all security portals.
RADIUS Server Timeout	Generated when the RADIUS server fails to respond within the RADIUS timeout period. The RADIUS server may be unreachable over the network, or the shared secret for the RADIUS server is incorrectly configured on the AP. If multiple RADIUS servers are configured in this authentication zone, the AP will switch to using the next one in the list.

Table 16: Airgo Access Point Alarms (continued)

Alarm ID	Description
Management User Login Success	Generated when a management user successfully logs in to the local AP.
Management User Login Failure	Generated when a management user fails to log in to the AP.
STA Failed EAPOL MIC Check	Generated when the MIC fails during EAPOL key exchange process. If the authentication type is WPA PSK and the failure happened during the pairwise key exchange, then the most likely reason is incorrect configuration of the WPA PSK on the station. It could also mean that an attacker's station is attempting to masquerade as a legal station.
STA Attempting WPA-PSK – No Pre-shared Key Is Set for SSID	Generated when a client station attempts to perform WPA-PSK-based authentication on a given SSID, but no WPA pre-shared key has been configured for that SSID.
Auth Server Improperly Configured on this SSID	Generated when the AP has determined that a station requires an authentication server, but none is configured for this SSID. Authentication servers are needed for EAP-based authentication and MAC address based ACL lookups.
STA Failed to Send EAPOL-Start	Generated when the AP has determined that a client station has failed to send an EAPOL-Start, possibly indicating incorrect configuration of the station. The AP expects the station to send an EAPOL-Start if the authentication type is deemed to be EAP-based. This can happen when WPA EAP authentication is negotiated, or when WEP is enabled on the AP and no manual WEP keys are configured.
RADIUS Sent a Bad Response	Generated during authentication when the RADIUS server sends a bad or unexpected response. This would occur if the cryptographic signature check failed or an attribute is missing or badly encoded.
RADIUS Timeout Too Short	Generated when the AP receives a late response from the RADIUS server, generally due to high network latency. The AP may have attempted multiple retries or may have switched to another RADIUS server by this time. If this alarm is generated repeatedly, it may be desirable to increase the timeout associated with the authentication server.
STA Authentication Did Not Complete in Time	Generated when the station authentication sequence did not complete in time.
Upstream AP Is Using an Untrusted Auth Server	Generated when the local BP determines that the upstream AP is using an untrustworthy authentication server. This could mean that the upstream AP is a rogue AP. If the downstream AP was previously enrolled in another network, it should be restored and re-enrolled in the new network.
Upstream AP Is Using a Non-portal Node As Its Auth Server	Generated when the local BP determines that the upstream AP is using a node that is not a security portal as its authentication server. The BP is aware of the other node, but does not believe it is authorized to be a security portal.
Upstream AP Failed MIC Check During BP Authentication	Generated when the MIC fails during the EAPOL key exchange process with a BP radio.

Table 16: Airgo Access Point Alarms (continued)

Alarm ID	Description
Premature EAP-Success Receive	Generated when an upstream AP sends an EAP success before authentication is complete. This may indicate that a rogue AP is trying to force an AP to join before authentication is complete.
Profile Not Configured for User-Group	Generated when the AP determines that the station is a member of a group that does not have a service profile defined for this SSID.
STA Has Failed Security Enforcement Check	Generated if the station attempts to use an encryption type that is not allowed in its service profile. The AP can advertise multiple encryption capabilities, but different stations may be restricted to different subsets of encryption capabilities based on their service profiles.
AP Detected Bad TKIP MIC	Generated when a bad TKIP MIC is detected on an incoming frame from a station that is encrypted with a pairwise/unicast key. All packets received by the AP are always encrypted with the pairwise/unicast key.
BP Detected Bad TKIP MIC on Incoming Unicast	Generated when a bad TKIP MIC is detected by a local BP radio on an incoming frame encrypted with the pairwise/unicast key.
BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast	Generated when a bad TKIP MIC is detected by a local BP radio on an incoming multicast or broadcast packet from the AP, where the packet is encrypted with the group/multicast/broadcast key.
STA Detected Bad TKIP MIC on Incoming Unicast	Generated when a bad TKIP MIC is detected by a station associated with this AP on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.
STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast	Generated when a bad TKIP MIC is detected by a station associated with a radio on an incoming multicast or broadcast packet from the AP, where the packet is encrypted with the group/multicast/broadcast key.
TKIP Counter-Measures Lockout Period Started	Generated when a TKIP counter-measures lockout period for 60 seconds is started. Indicates that the AP has determined that an attempt is underway to compromise the secure operation of TKIP. This happens if two MIC failures are detected within a 60-second interval. If this happens, the AP disassociates all stations and prevents new stations from associating for a period of 60 seconds.
EAP User-ID Timeout	Generated when a station fails to send its user-ID in time to complete its authentication sequence using the specified authentication type. The two authentication modes that require the station to send its user-ID are WPA EAP and legacy 8021.x for dynamic WEP. This alarm may indicate that a user prompt is not attended to on the client side.

Table 16: Airgo Access Point Alarms (continued)

Alarm ID	Description
EAP Response Timeout	Generated when a station fails to send an EAP Response in time to complete its authentication sequence using the specified authentication type and encryption. The two authentication modes that require the station to send EAP responses are WPA EAP and legacy 8021.x for dynamic WEP. This alarm may mean that a user prompt is not attended to on the client side. It may also indicate that the client silently rejected an EAP request sent from the RADIUS server – perhaps because it did not trust the RADIUS server's credentials.
EAPOL Key Exchange –Message 2 timeout	Generated when a station fails to send the WPA EAPOL-Key Pairwise Message #2 in time to complete the pairwise key exchange.
EAPOL Key Exchange – Message 4 timeout	Generated when a station fails to send the WPA EAPOL-Key Pairwise Message #4 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.
EAPOL Group 2 Key Exchange Timeout	Generated when a station fails to send the WPA EAPOL-Key Group Message #2 in time to complete its authentication sequence with a radio, using the specified authentication type and encryption.

Alarm Filter

Use the Alarm Filter tab (Figure 158) to eliminate selected events from the alarm displays in the Alarm Summary and Alarm Table tabs.

Select an event ID from the list, and click **Add** to include the event type in the list of events that are not reported. Each added event is included in the Event Filter Table Drop List at the top of the tab. The table includes the event ID and a description. To remove an event from the list, select the event, and click **Delete**.

Figure 158: Fault Management - Alarm Summary - Alarm Filter

The screenshot shows a web interface for configuring alarm filters. At the top, there are three tabs: 'ALARM SUMMARY', 'ALARM TABLE', and 'ALARM FILTER', with 'ALARM FILTER' being the active tab. To the right of the tabs are 'HELP' and 'CLOSE' buttons. Below the tabs, the breadcrumb 'Fault Management | Alarm Summary | Alarm Filters' is displayed with a double arrow icon. A text box contains the instruction: 'Configure critical events that should be filtered out of the system. These events will be dropped at the source (i.e., this AP) and will not be forwarded to any external Network Management System.' Below this is the 'Event Filter Table (Drop-List)' section, which contains a table with two columns: 'Event ID' and 'Event Description'. A 'DELETE' button is located below the table. The 'Add Events To Event-Filter-Table' section features a dropdown menu for 'Event ID' with 'BP authentication failed' selected, and an 'ADD' button below it.

ALARM SUMMARY ALARM TABLE ALARM FILTER HELP CLOSE

Fault Management | Alarm Summary | Alarm Filters ⇄

Configure critical events that should be filtered out of the system. These events will be dropped at the source (i.e., this AP) and will not be forwarded to any external Network Management System.

Event Filter Table (Drop-List)

Event ID	Event Description
----------	-------------------

DELETE

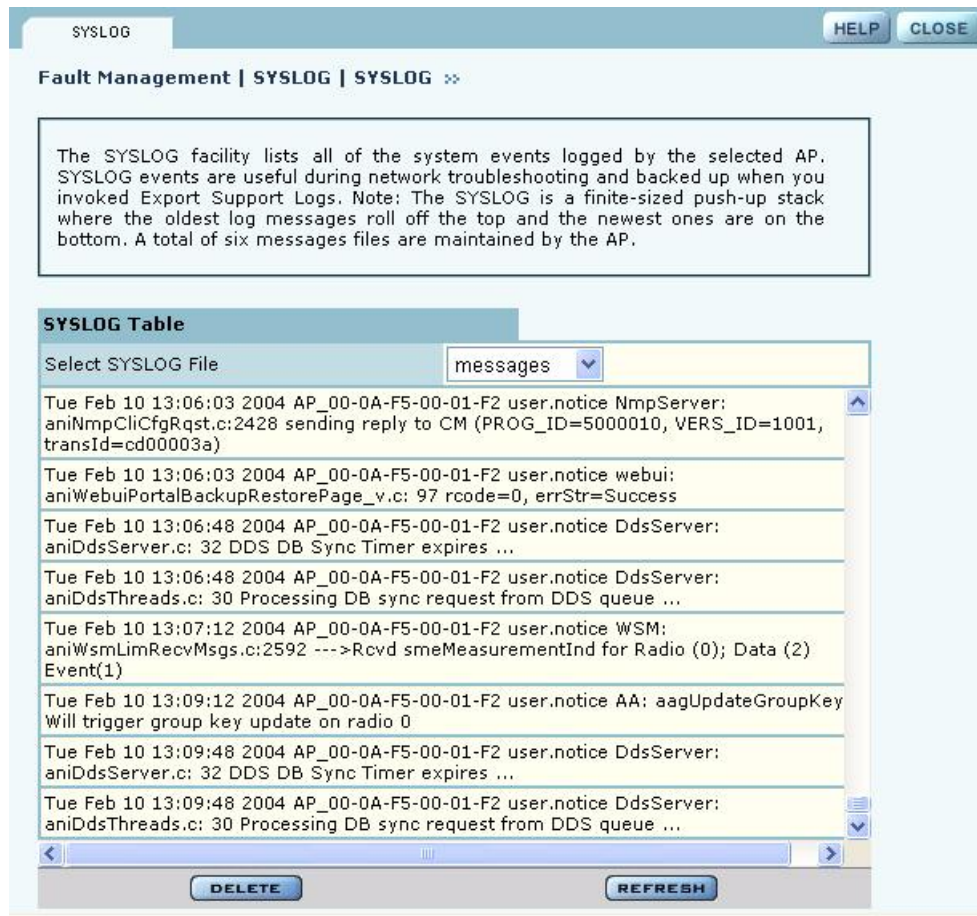
Add Events To Event-Filter-Table

Event ID: BP authentication failed

ADD

Viewing the Syslog

Select SYSLOG from the Fault Management menu to view syslog messages used for network troubleshooting. The most recent messages are in the default message file, *Messages*, with the latest messages at the top. To view older messages, select the appropriate message .x file from the list on the SYSLOG panel (Figure 159). See “Syslog Configuration” on page 241 for instructions on configuring the syslog message output.

Figure 159: Fault Management - SYSLOG

Using the Security Portal Menu

Use the Security Portal menu items to manage user access to the wireless network and to configure the RADIUS proxy feature.

Managing User Accounts

Choose **User Management** from the Security Portal menu to manage the authentication of users by way of the internal RADIUS database on the NM Portal AP. The panel contains the following tabs:

- Wireless Users — Manage users who seek access to the wireless network.
- Admin Users — Manage administrators responsible for the wireless network.
- MAC ACLs — Identify and manage users using the MAC addresses of their computers.
- Guest User — Set up automatic password generation for guest users. For a description of this tab, see “Configuring Guest Access” on page 167.

Adding Wireless Users

Choose **User Management** from the Security Portal menu to open the Wireless Users tab, which contains a list of current network users (Figure 160).

Figure 160: Security Portal - User Management - Wireless Users

WIRELESS USERS ADMIN USERS MAC ACLs GUEST USER HELP CLOSE

Wireless User details the identity of a new user that has been enrolled in the Portal's RADIUS database and unique digital certificate has been issued. User is required to download and install the new certificate on his/her wireless computer by following the certificate link below. Subsequently, wireless user will be authenticated by the Portal AP using this digital certificate.

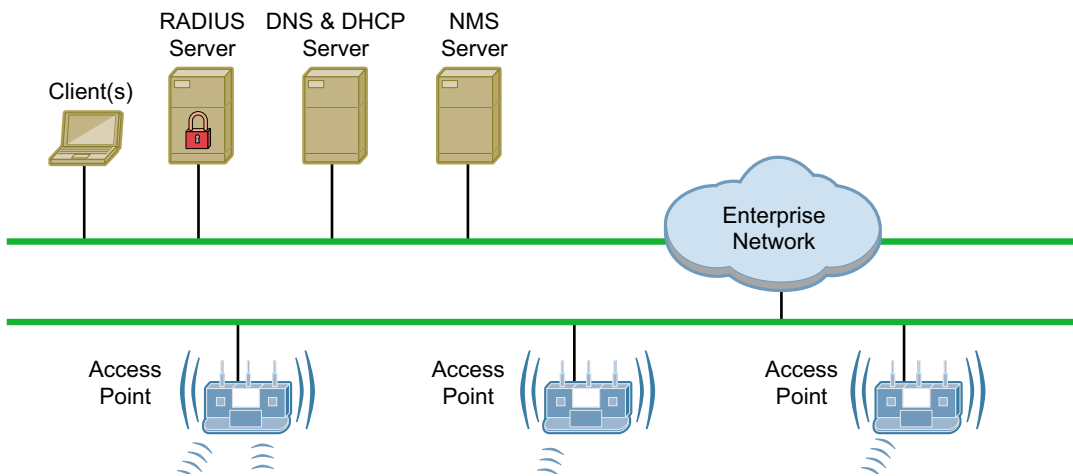
View Wireless User

Login Name	mlamb
User Group	employee
User First Name	Mary
User Last Name	Lamb
E-mail ID	mlamb@DeerCreekCo.com
Description	
User Password	CCK1Yt44
Certificate	Click here to download certificate.

< BACK

To add a new user, click **Add** to open the Add Wireless User entry panel (Figure 161).

Figure 161: Security Portal - User Management - Add Wireless User



Enter the following information:

Field	Description
Login Name	Assign a login name for network access (required).
User Group	Select a user group as defined in the RADIUS server.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Email ID	Enter the user's email address.
Description	Enter a text description, if desired.

Click **Add** to save the user record, **Reset** to clear the fields on the panel, or **Cancel** to return to the Wireless tab without saving the record.

When a wireless user is added to the database a unique certificate is generated for that user. The certificate must be installed on the user's PC. This can be done in one of two ways:

- Email — If an SMTP server is configured, the certificate is mailed to the user. To install the emailed certificate on the PC:
 - a Ask the administrator for the password associated with the certificate. This password is displayed in the user details page.
 - b Double click on the certificate obtained through email. When the certificate installation wizard asks for the password, supply the previously-obtained password.
- Download — To download the certificate:
 - a Click the Wireless Users tab to display the list of users.
 - b Click the login name link for the user, or highlight the checkbox to the left of the Login Name, and click **Details**. This opens the View Wireless User panel (Figure 162).
 - c Click the link entitled **Click Here to Download Certificate**. A security certificate pop-up opens with a prompt to open or save the certificate.
 - d Save the certificate on your local computer.

Figure 162: Security Portal - User Management - View Wireless User

WIRELESS USERS ADMIN USERS MAC ACLs GUEST USER HELP CLOSE

Wireless User details the identity of a new user that has been enrolled in the Portal's RADIUS database and unique digital certificate has been issued. User is required to download and install the new certificate on his/her wireless computer by following the certificate link below. Subsequently, wireless user will be authenticated by the Portal AP using this digital certificate.

View Wireless User

Login Name	mlamb
User Group	employee
User First Name	Mary
User Last Name	Lamb
E-mail ID	mlamb@DeerCreekCo.com
Description	
User Password	CCK1Yt44
Certificate	Click here to download certificate.

< BACK

Adding Administrative Users

To give designated users access to NM Portal or to the all APs in the network managed by this NM Portal, open the Admin Users tab (Figure 163).

Figure 163: Security Portal - User Management - Admin Users

WIRELESS USERS ADMIN USERS MAC ACLs GUEST USER HELP CLOSE

Security Portal | User Management | Admin Users >>

Add Administrator Users to Portal AP's RADIUS database for centralized management of admin login to all enrolled access-points. Admin Users are granted privileges to manage all enrolled access-points using either Web User-Interface (HTTPs) or CLI.

Network Admin User Table				
	Login ID	User Name	User Group	Last Modified Date
☐	alittle	Alice Little	Administrator	Thu Sep 9 06:06:38 2004

ADD DELETE MODIFY DETAILS

The tab opens with a list of current administrative users. To add a new user, click **Add**, and enter the following information in the Add Administrative User entry panel (Figure 164):

Field	Description
Login Name	Assign a login name for network access (required).
Password	Enter the password and enter it again in the Confirm Password field (required).
User First Name	Enter the first name of the user.
User Last Name	Enter the last name of the user.
Email ID	Enter the user's email address.
Description	Enter a text description.

Figure 164: Security Portal - User Management - Add Administrative User

Add Network Administrative User

Login Name * mgoose

Password *

Confirm Password *

User First Name M.

User Last Name Goose

E-mail ID mgoose@DeerCreekCo.com

Description

ADD RESET CANCEL

After entering the requested information, click **Add**.

From the user list, you can also delete an existing user, modify user information, or view the details in a read-only table.

Adding MAC-ACL Users

Use the MAC-ACL tab (Figure 165) to identify and authenticate users by the MAC address of the computer rather than by login. This type of authentication is generally used to accommodate legacy equipment that does not support user-based authentication. MAC addresses are checked when the SSID has MAC-ACL enabled and Open access, static WEP keys, or WPA-PSK encryption are used. For more information on security options, see Chapter 7, “Managing Security.”

Figure 165: Security Portal - User Management - MAC-ACLs

WIRELESS USERS ADMIN USERS **MAC ACLs** GUEST USER HELP CLOSE

Security Portal | User Management | MAC-ACLs

The MAC-ACL provides a means of identifying users by their wireless client's MAC Address. All the MAC-ACLs are recorded in this RADIUS database and centrally managed for the entire wireless network, thus reducing the complexity of maintaining them at each AP.

MAC-Address Access Control List

	MAC Address	User Name	User Group	Last Modified Date
☐	00:0a:f5:00:60:25	MAC0 User	employee	Thu Sep 9 06:11:12 2004

ADD DELETE MODIFY DETAILS

The tab opens with a list of current MAC-ACL users. To add a new user, click **Add** and enter the following information in the Add MAC Address Based User entry panel (Figure 166):

Field	Description
MAC Address	Enter the MAC address that uniquely identifies the device. Use the tab key to move between the successive two-character fields. (required)
User Group	Select a group from the list or create a new group.
User First Name	Enter the first name of the user.
User Last Name	Enter the last name of the user.
Email ID	Enter the user's email address.
Description	Enter a text description, if desired.

Figure 166: Security Portal - User Management - Add MAC Address User

Add MAC Address Based User	
MAC Address *	00-0A-F5-00-6D-10 e.g 0A:0B:0C:0D:0E:0F or 0A-0B-0C-0D-0E-0F
User Group	employee New User Group ☐
User First Name	MAC1
User Last Name	User
E-mail ID	mac1@DeerCreekCo.com
Description	
ADD RESET CANCEL	

Click **Add** after entering the requested information.

From the user list, you can delete an existing MAC-ACL user, modify user information, or view the details in a read-only table.

Managing Guest User Passwords

For optional generation of guest passwords automatically at set intervals, use the Guest User tab, as explained in “Guest Access Security” on page 176.

RADIUS Proxy

Radius Proxy is a way of simplifying configuration for the external RADIUS authentication of wireless clients. When you bootstrap an AP as an NM Portal, RADIUS proxy is enabled automatically. All APs enrolled by this NM Portal will have Radius Proxy turned on. RADIUS proxy reduces configuration requirements at the external RADIUS server, as the server must now establish trust only with the security portal, rather than with all enrolled APs.

RADIUS proxy should only be enabled or disabled from NM Portal. Do not enable RADIUS proxy on an individual AP if it is not enabled on the NM Portal. Perform changes to the RADIUS proxy configuration on the NM Portal and then distribute the changes to the other enrolled APs.

i NOTE: It is possible to turn off RADIUS proxy on individual APs. This may be useful for test purposes. Be aware that this setting will be overturned when a policy is pushed from the NM Portal.

When RADIUS proxy is enabled, all RADIUS authentication requests from APs are routed to the NM Portal. If the NM Portal is not available, then these requests are routed to a backup security portal.

When RADIUS Proxy is disabled, all APs forward their external RADIUS authentication requests directly to the configured external RADIUS server or servers. This requires that you enter configuration information on the RADIUS server or servers for each AP rather than for the NM Portal and security portals only.

i NOTE: To guard against a single point of failure, it is recommended that you configure a backup security portal in addition to the working security portal.

The RADIUS Proxy feature can reduce administrative effort in the following ways:

- It is not necessary to configure each AP with knowledge of each external RADIUS server.
- It is not necessary to configure the external RADIUS server with each AP as a RADIUS client.
- Any normal (non-portal) AP can have its IP address changed at any time.

RADIUS proxy must be enabled or disabled on a network-wide basis. If this is not done the following may result:

- Loss of external auth-zone information on all APs
- Loss of external auth-server information on non-security portal APs
- Need to reset the SSID and admin auth-zones portal authentication zones for the network to function properly.

Due to these potential effects, it is important to back up the configuration of all APs prior to enabling or disabling RADIUS proxy. See “Managing the AP Configuration” on page 245 for instructions on backing up the AP configurations.

When enabling RADIUS proxy, there are specific configuration requirements for the NM Portal AP that acts as the enrollment portal, the backup security portal, and other normal (non-portal) APs.

Configuration Requirements for Portal AP (running Enrollment Service)

The following steps are required at NM Portal when enabling RADIUS Proxy:

- 1 Back up Portal AP Configuration (recommended). See “Managing the AP Configuration” on page 245.
- 2 Configure the external RADIUS server (external authentication servers).
- 3 Enable RADIUS Proxy. See “Configuring RADIUS Proxy” on page 228.
- 4 Generate a default Policy. See “Define Policy” on page 198
- 5 Distribute the default policy to all APs. See “Distribute Policy” on page 199.

i NOTE: When RADIUS proxy is enabled, external authentication server information must NOT be deleted. This information is used by the RADIUS proxy server to proxy RADIUS authentication requests to these external RADIUS servers. Once RADIUS proxy is in effect, all future user authentication traffic is redirected to the proxy. In order to avoid disruption in user authentication, it is strongly recommended to nominate another AP to be a backup security portal.

If RADIUS proxy is turned off, it is necessary to rebind the authentication zones to the SSIDs. This can be accomplished from a restored backup configuration. Whenever the proxy state changes or the external auth server configuration changes, a new default policy must be regenerated and redistributed to all the enrolled APs.

When you enable RADIUS-proxy, the auth-zone setting is hidden because there are no external auth-zones being used on this AP. The auth-servers settings shows the list of internal and external RADIUS servers. You can edit the list of external RADIUS servers used by the proxy on this portal

and distribute the new list to one or more security portals if you generate a new default policy and distribute it.

For more information on SSIDs, authentication zones, and authentication servers, see “Configuring Authentication Zones” on page 155.

Configuration Requirements for Backup Security Portal

It is highly recommended that you configure one or more backup security-portals when configuring RADIUS proxy. Each of the backup security portals must establish trust with the external RADIUS servers. The synchronization of configured external RADIUS servers from the primary Security-Portal (usually the NM Portal AP) is automatic, and no special action is required by the user. All external RADIUS server configuration should be done on the NM Portal AP, not on the backup security portals.

Configuration Requirements for Normal APs (Non-Portal APs)

Configure RADIUS proxy on normal (non-portal) APs by defining a policy with RADIUS proxy and then distributing it to the normal APs. This ensures that the correct sequence of configuration changes are applied to the normal APs when RADIUS proxy is enabled or disabled.

When RADIUS proxy is enabled on a normal AP, all external auth-server information is deleted. Security is enhanced because the number of global secrets (such as Shared Secret between external RADIUS server and the AP) maintained on the normal APs is reduced. In addition, all SSID security is bound to the portal auth-zone (which is a list of security-portals in the network), permitting normal APs to redirect wireless authentication to security portal APs that take on the role of sending a proxy request to external RADIUS servers. Similar redirection occurs with administrator logins. To disable RADIUS-proxy on the normal AP, you must go back to the NM Portal AP, disable RADIUS proxy, and redistribute the policy to all APs across the network.

When RADIUS-proxy is disabled, then a policy push from the NM Portal AP to the normal APs restores the external RADIUS server configuration along with the corresponding shared secrets.

Configuring RADIUS Proxy

Use the RADIUS Proxy panel (Figure 167) in the AP web interface to enable the RADIUS proxy feature. For the full set of steps required to configure RADIUS proxy, see “Configuration Requirements for Portal AP (running Enrollment Service)” on page 227.

 **NOTE:** It is highly recommended that you make the decision to use RADIUS proxy when first configuring the network, in order to make the configuration seamless and less error prone. The RADIUS proxy setting should be made part of the default NM Portal or NMS Pro policy prior to enrolling other APs. This ensures that all subsequently configured APs inherit the correct proxy settings when they are enrolled.

Figure 167: RADIUS Proxy

RADIUS PROXY [HELP](#) [CLOSE](#)

Security Portal | RADIUS Proxy | RADIUS Proxy Configuration »

When Radius Proxy is enabled the first time, the security settings get re- configured to support radius proxying. In order to ensure that the new configuration is correctly distributed to all the enrolled nodes, please following the link at the bottom of the page to initiate the policy (configuration) distribution.

RADIUS Proxy Server Configuration

Enable Radius Proxy Server ☒

[APPLY](#)

Distribute Default Policy [GO >>](#)

Configure the following setting on this panel:

Item	Description
Enable RADIUS Proxy Server	Select the checkbox to enable the RADIUS Proxy server feature, and click Apply .

i **NOTE:** When RADIUS proxy is enabled, the authentication zone configuration is deleted. When APs are enrolled into the network, the configuration policy is distributed to the AP. If RADIUS proxy is turned off, then the authentication zone configuration must be re-added to the NM Portal and the default policy must be re-generated and distributed to the managed network to enable authentication services via an external RADIUS server. Moreover, the external RADIUS server must be re-configured to accept the individual APs as RADIUS clients.

Using the Mobility Services Menu

The Layer-3 Mobility feature provides seamless roaming for wireless clients in a wireless network in which there are multiple subnets in proximity to each other. An example of a network that requires seamless IP roaming is a multi-story building in which each floor is on a different subnet and wireless clients need to roam between floors without losing connectivity.

In contrast to Layer-3 roaming, Layer-2 roaming occurs by default when a wireless client roams between APs on the same subnet. Layer-2 roaming is automatically seamless if IAPP is configured in the network (see “Configuring Inter Access Point Protocol (IAPP)” on page 95). Across subnets, Layer-3 mobility is required to avoid the disruption of forced disassociation and reassociation as a client moves across subnet boundaries. With the Layer-3 Mobility feature, wireless clients move across subnets without a required IP address change, and application sessions (UPD, TCP, or HTTP) are uninterrupted.

Layer-3 Mobility is particularly useful in providing Wi-Fi VoIP services. For example, if a Wi-Fi VoIP phone must change its IP address during a conversation, the call is usually dropped. By

enabling retention of the same IP address, clients can continue their conversations without interruption.

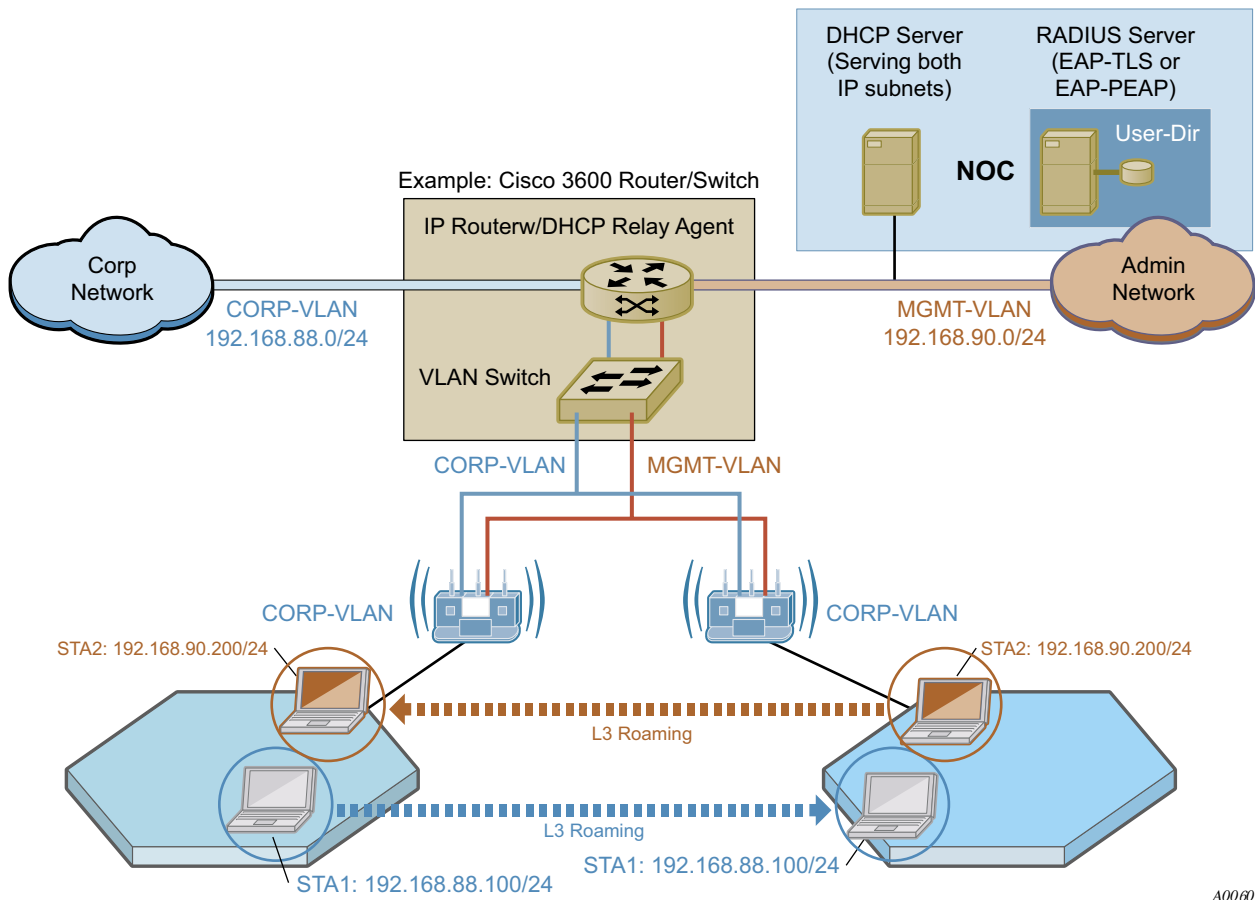
Layer-3 Mobility requires wireless client reauthentication, and delays can occur for some authentication methods. For example, if the clients use WPA-EAP for authentication, then Layer-3 roaming still requires clients to be reauthenticated by an external RADIUS server. Delays can occur while authentication messages are exchanged between the AP and the RADIUS server. However, if WPA-PSK or WEP methods are used for authentication, the client will be reauthenticated on the new AP to which it has roamed, thereby avoiding the latency introduced by the external RADIUS server.

When creating a Layer-3 Mobility zone, all APs should be managed by the same management domain (NMS Pro or NM Portal). There are two methods of configuring Layer-3 Mobility:

- Layer-3 Mobility Using VLANs (See “Layer-3 Mobility Using VLANs”)
- Layer-3 Mobility Using Tunneling (See “Layer-3 Mobility Using Tunneling”)

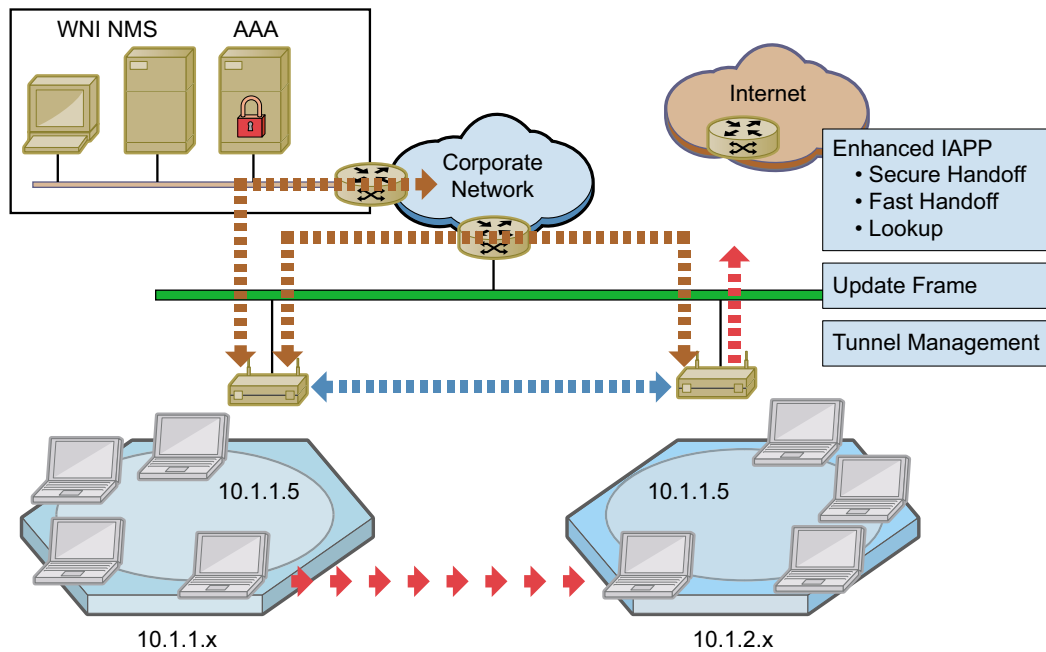
Layer-3 Mobility Using VLANs

This approach requires the use of VLANs to enable seamless Layer-3 Mobility. It is suitable for small networks with a number of subnetworks because traffic from all subnetworks is bridged by the APs in separate VLANs. Client stations roaming between APs are kept within the same VLAN and, hence, remain in a single subnet. Layer-3 mobility is supported with interface VLANs and user VLANs (Figure 168).

Figure 168: Layer-3 Roaming Using VLANs

Layer-3 Mobility Using Tunneling

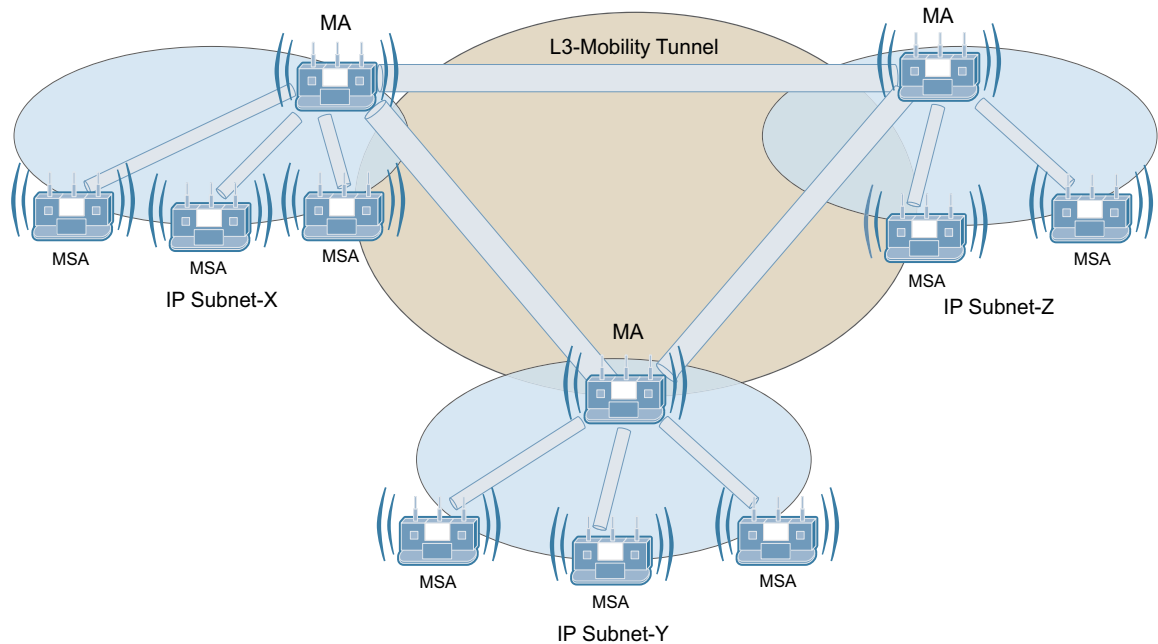
To use the tunneling approach for Layer-3 Mobility, it is necessary to have a network with multiple subnets in wireless proximity. When a client in a subnet moves to another subnet, a handshake takes place and a tunnel is created between the two APs (Figure 169).

Figure 169: Layer-3 Mobility - Tunnel Approach

A0057

The tunneling approach uses mobility agents (MAs) and mobility sub-agents (MSAs). Each MA configures a tunnel to every other MA in the network, thereby creating a fully meshed tunneled infrastructure to carry Layer-3 Mobility traffic between these subnetworks. There can only be one MA per subnet, and it is highly recommended that the AP you designate as MA be directly connected to the wired network (not a wireless-backhaul AP). All other APs in the subnetwork automatically assume the role of an MSA and forward their Layer-3 Mobility traffic to the MA in the same subnet. The MSAs do not need to be configured; they automatically bind to the MA, and it is the MA's job to periodically advertise itself to all APs on the subnet (See Figure 170).

NOTE: If the MA is in the process of booting when a client station is already associated with the MSA, then the station cannot roam successfully on its first attempt. Subsequent roaming attempts should succeed.

Figure 170: Layer-3 Mobility - Mobility Agents and Sub-Agents

A0061

The wired network AP that is selected as an MA must be attached to one of the following:

- Ethernet switch that supports jumbo frames (>1518 bytes). The switches must pass through tagged VLAN packets.
- VLAN enabled Ethernet switch that supports switching of VLAN tagged frames. Such VLAN switches do require configuration to support Layer-3 Mobility.

The following restrictions apply to Layer-3 Mobility using tunneling:

- Redundancy: There can be only one AP per subnet designated as the MA. If the designated MA is not operational, it is necessary to manually configure another MA.
- Maximum number of IP subnets: Layer-3 mobility can be configured with a maximum of 16 subnets.
- Management: All APs involved in a Layer-3 mobility configuration must be managed by the same network management solution (NM Portal or NMS Pro).
- SSID: All the APs in a Layer-3 mobility configuration must be configured with the same SSID.

Mobility Configuration Tab

Use the Mobility Configuration tab (Figure 171) to enable mobility support and add mobility agents.

Figure 171: Mobility Configuration

MOBILITY-CONFIG ROAM-STATIONS ROAMING-STATS TUNNEL-STATS HELP CL

Mobility Services | L3 Mobility | Mobility Configuration >>

Mobility Support can be configured from this page. User can also see & update the mobility Agent table. User can also see & update the mobility Agent table.

L3 Mobility Configuration

Enable L3 Mobility (Tunneling) ☒ Yes ☐ No

APPLY RESET

Select Mobility Agent (Wired AP)

	AP Name	IP Subnet	AP Device ID
☐	192.168.91.1/24	255.255.255.0	AP_00-0A-F5-00-00-D5
☐	192.168.91.26/24	255.255.255.0	AP_00-0A-F5-00-01-86
☐	192.168.90.48/24	255.255.255.0	AP_00-0A-F5-00-08-28

ADD

Mobility Agent Table

	AP Name	AP Device ID	Mobility IP Subnet
☐	192.168.91.1/24	AP_00-0A-F5-00-00-D5	192.168.91.0
☐	192.168.90.48/24	AP_00-0A-F5-00-08-28	192.168.90.0

DELETE DELETE ALL

This tab contains the following information and settings:

Item	Description
Enable L3 Mobility (Tunneling)	Choose Yes to activate the L3 mobility capability, and click Apply . Click Reset to return to the previously saved value.
Select Mobility Agent (Wired AP)	Select an AP and click Add to enroll the AP as a mobility agent. NOTE: Only one AP in a subnet can be designated as a Mobility Agent.
Mobility Agent Table	View the list of currently assigned mobility agents. To delete an agent: - Choose the entry and click Delete. Click OK to confirm. To delete all currently assigned agents: - Click Delete All. Click OK to confirm.

Roaming Stations Tab

When client stations roam across subnets, the MA and the MSAs in the subnet track their movement. The Roaming Stations tab (Figure 172) shows the set of stations that have roamed to the selected subnet.

Figure 172: Mobility Configuration - Roaming Stations

MOBILITY-CONFIG ROAM-STATIONS ROAMING-STATS TUNNEL-STATS HELP CLOSE

Mobility Services | L3 Mobility | Roamed Stations >>

When stations roam across subnets, they are tracked by the Mobility Agent for that subnet. The table below shows the set of Stations that have roamed to the selected subnet.

Select Mobility Agent(s) All-MAs

Home IP Subnet	Roamed IP Subnet	MA IP Address	AP Interface	STA MAC Address	STA Assoc Duration
192.168.90.0	192.168.91.0	192.168.91.1	wlan0	00:0a:f5:00:05:dd	Days:49693, Hrs:11, Mins: Secs:28

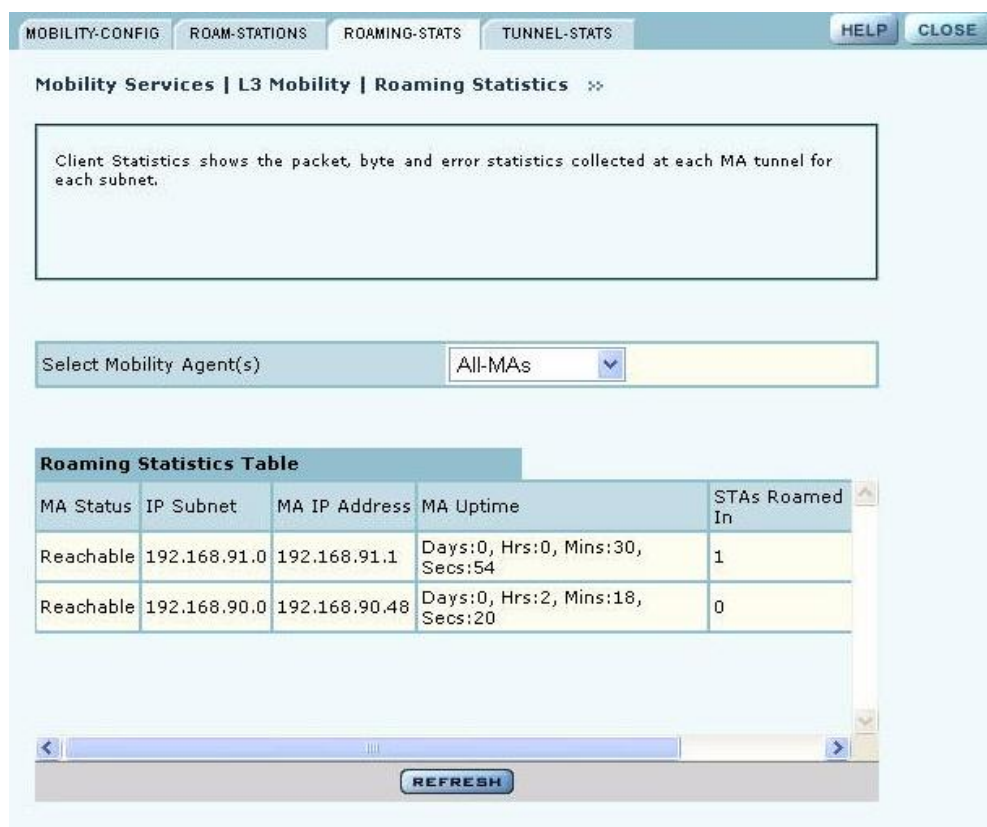
REFRESH

The table on this panel contains information for the subnet or subnets indicated by the Mobility Agent (or all Mobility Agents) selected from the pull-down list. The table lists the following information for each client station:

Item	Description
Home IP Subnet	Subnet in which the client was originally associated
Roamed IP Subnet	Subnet to which the client has roamed
MA IP Address	IP address of the MA or MSA to which this station is associated
AP Interface	Radio interface at the MA or MSA to which the station is associated
STA MAC Address	Client's MAC Address
STA Assoc Duration	Length of time in the client has been associated with the MA or MSA

Roaming Statistics Tab

The Roaming Statistics tab (Figure 173) displays roaming activity for each MA.

Figure 173: Mobility Configuration - Roaming Statistics

The table on this panel contains information for the subnet or subnets indicated by the Mobility Agent (or all Mobility Agents) selected from the pull-down list. Each row lists the following information for a client station:

Item	Description
MA Status	Indication of whether the MA is reachable or not (if not reachable, then stations that roamed to that subnet are able to tunnel traffic out of that subnet)
IP Subnet	Subnet for which the statistics are being displayed
MA IP Address	IP address of the MA in that subnet
MA Uptime	Amount of time the MA has been powered up and operational (Days: Hours: Minutes: Seconds)
STAs Roamed In	Sum of the number of stations that have roamed into this subnet as reported by the MA and MSAs combined
STAs Roamed Out	Sum of the number of stations that have roamed out of this subnet to other subnets as reported by the MA and MSAs in this subnet

Tunneling Statistics Tab

The Tunnel Statistics tab (Figure 174) shows the packet, byte, and error statistics collected at each MA tunnel for each subnet.

Figure 174: Mobility Configuration - Tunnel Statistics

MOBILITY-CONFIG ROAM-STATIONS ROAMING-STATS TUNNEL-STATS HELP CLOSE

Mobility Services | L3 Mobility | Tunnel Statistics >>

The Table below shows the Mobility Statistics details for a selected Mobility Agent.

Select Mobility Agent(s) All-MAs

MA IP Address	Tunnel Local IP Subnet	Tunnel Remote IP Subnet	Tunnel Interface	Received Bytes	Received Pkts	Transmit Pkts	Transmit Bytes
192.168.91.1	192.168.91.0	192.168.90.0	gre1	125442	1840	1251	123
192.168.90.48	192.168.90.0	192.168.91.0	gre2	504018	6808	11541	108

REFRESH

The following information is presented for each Mobility Agent selected from the pull-down list:

Item	Description
MA IP Address	IP address of the selected mobility agent
Tunnel Local Subnet	Subnet address of the tunnel endpoint terminating on the selected Mobility Agent
Tunnel Remote Subnet	Subnet address of the tunnel endpoint terminating on a remote Mobility Agent
Tunnel Interface	Name of the tunnel connecting the remote and local subnets on the selected Mobility Agent
Received Bytes	Number of bytes received by the tunnel interface on the selected Mobility Agent
Received Pkts	Number of packets received by the tunnel interface on the selected Mobility Agent
Transmit Pkts	Number of packets transmitted by the tunnel interface on the selected Mobility Agent
Transmit Bytes	Number of bytes transmitted through the tunnel interface on the selected Mobility Agent
Received Multicast	Number of multicast packets received through the tunnel interface on the selected MA

Item (continued)	Description
Received Error Packets	Packets with errors received through the tunnel interface on the selected MA
Received Drop Packets	Number of received packets dropped by the tunnel interface
Misaligned Packets	Always equal to 0
FIFO Errors	Always equal to 0
Transmit Error Packets	Number of packets dropped due to inability to find the route
Transmit Drop Packets	Number of packets dropped by the tunnel interface upon transmission due to system congestion

10 Maintaining the Access Point

A variety of tools are available to maintain the Airgo Access Point.

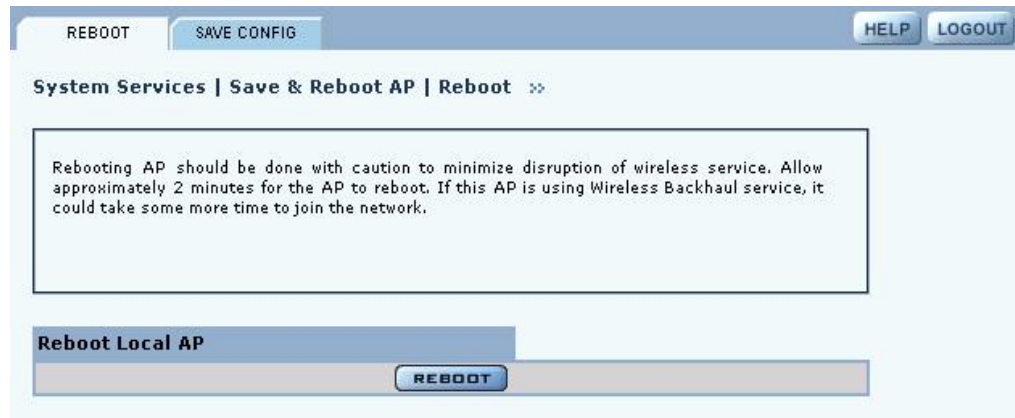
This chapter describes the tools in the following sections:

- [Rebooting the AP](#)
- [Saving the AP Configuration](#)
- [Managing the System Configuration](#)
- [Managing the AP Configuration](#)
- [Upgrading Software](#)
- [Common Problems and Solutions](#)

Rebooting the AP

Choose **Save & Reboot AP** from the System Services menu to open the Reboot Configuration panel. To begin the process, click **Reboot** (Figure 177). The process takes approximately two minutes, and may take additional time if the AP is currently used for wireless backhaul service.

Figure 175: System Configuration - Reboot AP



Saving the AP Configuration

Choose **Save & Reboot AP** from the System Services menu, and then click **Save Config** to open the Save Configuration tab (Figure 177).

To save the current AP configuration, click **Save Configuration**.

To enable global save, click **Apply**.

Figure 176: System Configuration - Reboot AP

REBOOT SAVE CONFIG HELP LOGOUT

System Services | Save & Reboot AP | Save Configuration >>

Enable global save operation after every "apply" button click. Also user can save current configuration now itself.

Save Configuration Option

Auto Save Configuration After Every 'APPLY' Button is Clicked ☒ Enable

APPLY SAVE CONFIGURATION

Managing the System Configuration

Choose **System Configuration** from the System Services menu to access the network-related configuration features of the Airgo AP and set up syslog parameters.

The panel includes the following tabs:

- IP Configuration — Configure IP and host settings.
- Syslog Configuration — Set up and view the syslog.
- License Management — Configure additional licenses on the AP.
- NMS Configuration — Specify the entities used for network management, including the NMS Pro server and NM Portal AP.
- Hardware Options — Enable the real-time clock and buzzer.

IP Configuration

Use the IP Configuration tab (Figure 177) to update the IP and basic system configuration for the Airgo AP.

Figure 177: System Configuration - IP Configuration

IP CONFIG

SYSLOG CONFIG

LICENSE MGMT

NMS CONFIG

HW OPTIONS

HELP

LOGOUT

System Services | System Configuration | IP Configuration >>

Configure AP identity information, such as its Hostname, IP address, DNS server, Gateway IP address, AP location, administrator contact (email-address), etc. NOTE: AP requires a stable management IP address assignment (either via DHCP server or static IP configuration).

Management IP Configuration

DHCP Assigned IP Address

☒ Enable

DNS IP Address *

192.168.168.1

Management IP Address/Maskbits *

192.168.168.24/24

Gateway IP Address *

192.168.168.254

APPLY

RESET

System Identity Configuration

Host Name *

AP_00-0A-F5-00-01-F2

AP Location

Floor 1 South

Administrator Contact

admin@DeerCreekCo.com

APPLY

RESET

The tab is divided into two sections. Click **Apply** after configuring each section, or **Reset** to return to the default values. Configure the following fields:

Field	Description
DHCP Assigned IP Address	Enables the AP to obtain an IP address for the AP from the network DHCP server.
DNS IP Address	Enter the IP address of the DNS server. (required)
Management IP address /Maskbits	Enter the IP address and subnet prefix of the management server. (required)
Gateway IP address	Enter the IP address of the network gateway. (required)
Host Name	Enter a unique name for the AP. The default is the device ID, which is derived from the MAC address. (required)
AP Location	Enter a text description of the physical location of the AP.
Administrator Contact	Enter the contact information for the administrator.

Syslog Configuration

Syslog tracks and records information about network activities for later viewing and analysis.



CAUTION: Only an authorized administrator should change syslog levels or enable or disable syslog capabilities. Arbitrary changes to syslog can adversely affect the AP.

The top area of the Syslog panel (Figure 178) provides controls to set the logging level and scope for a variety of functional areas or modules.

Figure 178: System Configuration - Syslog Configuration

System Services | System Configuration | SYSLOG Configuration »

SYSLOG is a multi-purpose logging facility and provides vital information about salient events, errors, and debug logs. By default, a SYSLOG server runs on a portal AP to collect events from other enrolled APs. If you use a remote SYSLOG server, then the portal AP will not be able to manage faults for that AP. NOTE: Do not change log levels during normal AP operations.

SYSLOG Configuration

SYSLOG Level * Level: emergency Module: all-modules

Remote SYSLOG Logging * ☐ Enable

Remote SYSLOG Server *

APPLY RESET

Module SYSLOG-level Details

Module	SYSLOG-level
networking	notice
security	notice
radio	notice
discovery	notice
fault	notice
enrollment	notice
sw-download	notice
dds	notice
cm	notice

The tab contains the following settings:

Field	Description
Syslog Level	Select the activity level that triggers a syslog entry. Choose from several levels (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug). (required)
Syslog-Level Module	Select whether to record a specific type of activity, or include all the activities in the list. (required)
Remote Syslog Logging	Indicate whether to enable a remote server to monitor events across the network.
Remote Syslog Server	If the Syslog server is enabled, enter the remote server hostname or IP address.
Remote Syslog Server Port	If the Syslog server is enabled, enter the IP address or hostname of the server port. (optional)

License Management

Use the License Management tab (Figure 179) if it is necessary to change the license key for the AP. Enter or verify the license key for the AP, and click **Apply**. Click **Reset** to clear the field.

Figure 179: System Configuration - License Management

The screenshot shows the 'License Management' tab selected in the 'System Configuration' section. The interface includes a breadcrumb trail: 'System Services | System Configuration | License Management'. A text box contains the instruction: 'License keys can enable new features. Please consult your users guide to determine if additional features can be added to this AP.' Below this, the 'License Configuration' section has a label 'Add License Key *' and a text input field containing 'LQ6E-NX6K-QT3X'. A hint below the field reads 'e.g. T6PR88GJRHKC or T6PR-88GJ-RHKC'. At the bottom of this section are 'APPLY' and 'RESET' buttons.

NMS Configuration

Use the NMS Configuration tab (Figure 180) to identify network management servers and to determine which network management system will receive fault and event notifications.

NOTE: If the AP is already enrolled, it is not necessary to modify the settings on this panel. However, adding IP address does not automatically allow NM Portal or NMS to manage the AP. The AP must be enrolled to be managed.

Figure 180: System Configuration - NMS Configuration

System Services | System Configuration | NMS Configuration ⇄

This AP can be managed by either an external Network Management System (NMS), a portal AP or both. NMS is always designated as a primary manager; whereas portal AP is always designated as an auxiliary manager. When both managers manage an AP, then the auxiliary manager subordinates to the primary manager. NOTE: IP addresses of primary and auxiliary NMS are auto-configured.

NMS Configuration

Primary Manager IP Address	Unavailable
Auxiliary Manager IP Address	192.168.74.253

APPLY **RESET**

Enter the following values to set the NMS configuration:

Field	Description
Primary Manager IP Address	Enter the IP address of the NMS server responsible for managing the AP.
Auxiliary Manager IP Address	If applicable, enter the IP address of the NM Portal AP used to manage the AP at the branch location (in conjunction with an NMS Pro server as a primary manager).

Click **Apply** to save the entries or **Reset** to return to the previously saved values.

Hardware Options

Select **HW Options** (Figure 181) to set the buzzer and the real-time clock (RTC), which keeps track of the date and time in the event that the AP loses power. This feature is not required if the AP is always connected to the Internet.

Figure 181: System Configuration - Hardware Options

System Services | System Configuration | Hardware Options »

AP is optionally equipped with Real-Time-Clock (RTC) and Buzzer. It is recommended to enable RTC as it will preserve the clock setting even when the AP is powered down. Buzzer facility alerts you when AP needs administrator attention; however it can be muted by disabling it.

Real Time Clock Configuration

Enable Real Time Clock ☒

APPLY **RESET**

Buzzer Configuration

Enable Buzzer (disable to mute) ☒

APPLY **RESET**

Select the following parameters on this tab

Field	Description
Enable Real Time Clock	Use the real-time clock (RTC).
Enable Buzzer	Activate the AP buzzer to locate the AP, if necessary.

Click **Apply** to save the entries or **Reset** to return to the previously saved values.

Managing the AP Configuration

Choose **Configuration Management** from the System Services menu to open the Configuration Management feature panel. The panel contains the following tabs:

- **Secure Backup** — Use https to perform a secure backup of the AP configuration.
- **Configuration Backup** — Back up and restore configurations, export log files, and reset the AP configuration to the factory defaults.
- **Configuration Reports** — View configuration reports for the AP.
- **Reset Configuration** — Revert to the factory default configuration, or reset specific subsystems to default configuration.

Secure Backup

Perform the following functions on the Secure Backup tab (Figure 185):

Task	Steps
Back up the AP configuration using https	1 Click Save Configuration. 2 When the configuration is generated, a hyperlink is displayed. Right-click and select Save As to save the configuration locally. 3 After the configuration file is saved, click Delete to remove the file from the AP. The file takes up space in AP persistent storage, so it is recommended that you remove it.

Task	Steps
Restore the AP configuration	1 In the Restore Configuration area, click Browse and select the configuration file. 2 Click Apply to restore the configuration and reboot the AP. NOTE: If the AP has been unenrolled or restored to factory defaults, it is not possible to reapply the configuration using this method. The AP must be reenrolled and have a new configuration created.
Generate support logs	1 Click Generate Support Logs. 2 When the configuration is generated, a hyperlink is displayed. Right-click and select Save As to save the configuration locally. 3 After the support logs file is saved, click Delete to remove the file from the AP. The file takes up space in AP persistent storage, so it is recommended that you remove it.

Figure 182: Configuration Management - Secure Backup

SECURE BACKUP CONFIG REPORT RESET CONFIG TFTP BACKUP HELP LOGOUT

System Services | Configuration Management | Secure Backup »

It is recommended to backup AP configuration periodically. When required, restore AP configuration using the backup copy and reboot the AP. During technical support you will be asked to export support logs and send them to a technical support organization. NOTE: Delete temporary files after uploading to your client PC.

Backup AP Configuration

Save Current Configuration

Click Link to Download Configuration [apconfig.xml](#) **DELETE**

Restore AP Configuration

From file **Browse...**

APPLY **RESET**

Export Support Logs

Generate Support Logs **GENERATE**

Click Link to Download Logs

Secure Backups with NM Portal

Each NM Portal contains network and security databases in its persistent storage that should be backed up periodically. Note that the Secure Backup function backs up only the configuration file of the AP, whereas the secure backup capability in the NM Portal Network Management explorer allows you to back up the security databases along with the configuration of the AP.

If an NM Portal AP must be reset to factory defaults on a network with existing enrolled APs, follow these steps to restore the Portal AP:

Condition	Action
A backup of the NM Portal AP exists and the AP is functional	After resetting the Portal AP to factory defaults, bootstrap the AP as the NM Portal. Make sure the AP is assigned the same IP address it had originally. Restore the NM Portal Backup to the same AP. This should restore the portal to its configured state.
A backup of the NM Portal AP exists but the AP is not functional	Use a functioning AP that has been reset to factory defaults and make sure that this AP obtains the same IP address as the original NM Portal AP. Bootstrap this AP as NM Portal and restore the portal backup. This should produce a portal in the original configured state.
A backup of the NM Portal AP does not exist	1 Use an AP that is functional. 2 Reset it to factory-defaults. 3 Bootstrap it as a Portal AP. 4 Reconfigure the Portal AP to the desired settings. 5 Generate the Default Policy. 6 Reset all other enrolled APs to factory defaults and re-enroll them in the Portal AP. This would ensure that all re-enrolled APs obtain the same default policy.

Configuration Reports

Select any of the following configuration reports on this tab (Figure 183):

Report	Description
startup-config	Provides details on the configuration that is stored on the AP flash device and used each time the AP reboots.
running-config	Provides details on the current AP configuration, which may or may not match the startup configuration.
default-config	Lists the factory default settings shipped on the AP.

Click **Refresh** to update the selected report

Figure 183: Configuration Management - Configuration Reports

SECURE BACKUP CONFIG REPORT RESET CONFIG TFTP BACKUP HELP LOGOUT

System Services | Configuration Management | Configuration Reports »

Browse configuration reports of this AP. 'Startup' configuration is persisted on AP's flash device and used each time an AP reboots. 'Running' configuration is current state of system configuration which may not have been saved to flash. 'Default' configuration is what this AP has been shipped with.

Configuration Reports

Select Report: running-config

config backhaul uplink-criteria	
interface	wlan0
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-cost
interface	wlan1
ssid	DeerCreekCo
ipnetaddr	0.0.0.0/0
path-selection	lowest-weighted-cost
config radio network-density	
network-density	low
config radio channel	
interface	wlan0
periodic period	30

REFRESH

Reset Configuration

Use the Reset Configuration tab to reset the AP configuration or revert to the defaults for individual subsystems (Figure 184).

Figure 184: Configuration Management - Reset Configuration

System Services | Configuration Management | Reset Configuration »

Reset AP's startup configuration to defaults, while preserving its identity configuration (such as IP address, hostname, security setting, and enrollment state). Reset AP to factory default settings, which brings AP to pristine state. Reset only specific subsystem configuration, as required.

Reset Configuration To Default

Startup Configuration	RESET TO DEFAULT
All Configuration & Databases	RESET TO FACTORY DEFAULT

Reset Subsystems to Defaults

ap-quick-start	☐
backhaul	☐
bridge	☐
dhcp-server	☐
diagnostics	☐
filter	☐
guest-access	☐
interface	☐
ip-routing	☐
portal	☐
qos	☐
radio	☐
security	☐
snmp	☐
ssid	☐
system	☐
vlan	☐

RESET TO DEFAULT

Perform the following functions on this tab:

Function	Description
Reset Configuration to Default	1 Click Reset to Default or Reset to Factory Defaults. 2 Click Apply to reboot the AP with the selected configuration.
Reset Subsystems to Defaults	1 Select one or more individual subsystems to reset. 2 Click Apply to reboot the AP with the selected defaults.

Click **Reset** to clear the selections on the tab.

TFTP Backup

Use the TFTP Backup tab (Figure 185) to back up and restore configurations on an external TFTP server. Perform the following functions on this tab:

Task	Steps
Save configuration	1 Indicate whether to save the AP configuration each time a Save operation is done. 2 Click Apply. Click Save Configuration to save the current settings on demand.
Back up the configuration to a TFTP server	1 Enter the IP address of the TFTP server. 2 Enter or confirm the configuration file name. 3 Click Apply to restore the configuration and reboot the AP. NOTE: If the AP has been restored to factory defaults, it is not possible to reapply the configuration using this method. The AP must be reenrolled and a new configuration created.
Restore the configuration	1 Enter the IP address of the TFTP server. 2 Enter or confirm the name of the configuration file. 3 Click Apply.
Export support logs	1 Enter the IP address of the TFTP server. 2 Enter or confirm the name of the log file. 3 Click Apply.

The Reset buttons on the panel clear the field entries in the associated section.



NOTE: When you use a TFTP-based software download or restore backed-up configuration, use caution to select the correct file. If a very large file is chosen for download, then the TFTP client on the AP may consume all available free memory. If the correct file is chosen, AP performs a consistency check prior to consuming the file and saving it in the AP.

Figure 185: Configuration Management - TFTP Backup

System Services | Configuration Management | TFTP Backup »

The AP's configuration can be backed up to and restored from an external TFTP server. For technical support, use Export Support Logs feature to zip up all the relevant diagnostic log files and version information and make it available to your technical support organization.

Save Configuration Option

Auto Save Configuration After Every 'APPLY' Button is Clicked ☒ Enable

APPLY SAVE CONFIGURATION

Backup Configuration

TFTP Server * 192.168.168.1

To File apconfig.xml

APPLY RESET

Restore Configuration

TFTP Server *

From File apconfig.xml

APPLY RESET

Export Support Logs

TFTP Server *

To File supportLogs.tar.gz

APPLY RESET

Upgrading Software

From the NM Portal web interface, you can upgrade the software on enrolled APs throughout the network in one operation. You can also upgrade any individual, non-portal AP from the AP web interface. The same interface is used for both situations; however, access to the interface is different for an NM Portal than for a non-portal AP.

- If the AP is an NM Portal, click **Manage Wireless Network** to open the NM Portal interface, and then choose **Admin Tools > Software Upgrade** to open the Software Upgrade panel (Figure 186).
- If the AP is a non-portal AP, choose **Admin Tools > Software Upgrade** to open the Software Upgrade panel.

NOTE: The AP license file is not affected by software upgrades. The existing software license remains valid after the AP software is upgraded.

Figure 186: Software Upgrade

SW - UPGRADE HELP

Admin Tools | Software Upgrade

Upgrading a software image to a Portal AP requires three steps: 1) Download the software image via Web to stage it on Portal AP. 2) Select the APs to upgrade. 3) Distribute the image. NOTE: If you are upgrading from a TFTP server or upgrading a single non-Portal AP, only download (step 1) is required to upgrade image.

Software Image Upgrade

Select Software Image to Download to AP Browse...

DOWNLOAD

Software Download via TFTP

TFTP Server Name

Image File Name to Download to AP

APPLY RESET

The Software Upgrade panel offers two upgrade options. The Software Image Upgrade option uses https to download the software image to the AP. The Software Download via TFTP option uses TFTP to download the software image. Select only one of these options; it is not possible to use both methods at the same time.

The software upgrade process for an NM Portal consists of the following three steps:

Step	Description
Staging	The software image is downloaded to the Airgo AP.
Selection	APs are selected for software upgrade.
Distribution	The software upgrade image is distributed to the selected APs and installed. The AP is then rebooted.

If you are upgrading a non-portal AP or using TFTP as the download method, then the staging, selection, and distribution steps happen as a single process that cannot be interrupted once it begins. If you use the Software Image Upgrade selection in NM Portal, then staging, selection, and distribution are separate steps that can be monitored and canceled if needed.

Software Image File

The AP software image file conforms to a specific format that uses the filename extension `.img`. During download, the filename extension and structure are verified and the download is stopped if a problem with the file is detected.

Upgrading the AP Software

This section provides information for upgrading AP software using both the TFTP and https software download options. It is important to perform software upgrades during a scheduled maintenance window. Upgrading takes approximately four to five minutes per AP, and upgrading multiple APs from an NM Portal is a serial process. To manage system resources during a software

upgrade, the AP shuts down some services (such as CLI sessions) to create temporary memory and to validate the image prior to writing to AP's flash.

NOTE: When you distribute software from NM Portal to enrolled APs, the software distribution retries three times on each of the APs selected. Some management services on the NM Portal AP are shut down to make room for the new image distribution. The NM Portal AP runs through entire list of selected APs before it restarts management services. Therefore, it is best to perform software distribution when it is least disruptive to the network. Each AP upgrade can take up to two to three minutes.

Since NM Portal restarts services only after distribution is complete, you must explicit reboot the NM Portal if software distribution is interrupted.

CAUTION: Do not leave the Software Upgrade panel while download is taking place. If you click on another menu item during download, the download process is canceled.

Upgrade Using https Download - Individual Non-Portal AP

To upgrade a non-portal AP using https download:

- 1 Choose **Admin Tools > Software Upgrade**.
- 2 Browse to select the `.img` software image file.
- 3 Click **Download**.

A confirmation dialog appears asking you to confirm the software download.

- 4 Click **OK**.

The software image is downloaded to the AP, the AP software image is upgraded, and the AP is automatically rebooted.

Upgrade and Distribution Using https Download - NM Portal AP

To upgrade APs from NM Portal using https download:

- 1 Choose **Admin Tools > Software Upgrade**.
- 2 Browse to select the `.img` software image file.
- 3 Click **Download**.

A confirmation dialog asks you to confirm the software download.

- 4 Click **OK**.

The system verifies the filename extension and header information. When successful, the Software Download Status panel opens (Figure 187). Staging is now complete.

- 5 Select the APs to receive the upgrade.

- 6 Click **Distribute**.

A confirmation dialog asks you to confirm that the upgrade should now begin.

- 7 Click **OK**.

Figure 187: Software Upgrade - Download Status

SW - UPGRADE [HELP] [CLOSE]

Admin Tools | Software Download Status ✕

Distribute software image to one or more enrolled APs, including this Portal AP. Software distribution will take about 2 minutes per AP and proceeds serially with one AP at a time. It will retry to distribute the image 3 times on AP till it succeeds. When Portal AP (this AP) is part of the selection list, the image is written to flash last.

Current Image Details

Image Name	img.2286.1m.img
Image Info	0.7.0, build A.2286, AGN1dev, Deer Creek Company, Inc.,

Select APs for Image Distribution

☐	AP Name	AP Type	Compatibility	Download State
☐	192.168.75.230	Portal	Yes	Not Scheduled
☐	192.168.88.101	Non-Portal	Unknown	AP Not Reachable

[DISTRIBUTE] [CANCEL ALL]

The software distribution process begins by sending the software to the first selected AP. As soon as this AP receives the software, it upgrades its image and reboots automatically. The process then moves to the next selected AP. After all the APs have been upgraded, the NM Portal AP is upgraded and rebooted. The administrator must again log in to the NM Portal web interface after an upgrade and reboot.

Upgrade Using TFTP Download

To upgrade an NM Portal or non-portal AP using TFTP download:

- 1 Choose **Software Upgrade** from the Admin Tools menu.
- 2 Enter the IP address of the TFTP server.
- 3 Enter the name of the image file on the TFTP server. The default file is `target.ppc.ani.img`, under the boot directory of the TFTP server. Relative paths can be used when specifying the file name.
- 4 Click **Apply**.
A pop-up message asks for confirmation that you want the upgrade to begin.
- 5 Click **OK**.

The download process begins. Every 10 seconds the screen is updated with new status information. If the download is successful, the AP is automatically rebooted with the new software image. If the download is unsuccessful, an explanatory message is displayed in the Download Status column.

Canceling a Distribution

To cancel software distribution at any time, you must click **Cancel All**. This cancels distribution to APs that have not yet been upgraded, restarts services that were shut down during the upgrade, and removes the image file from the AP RAM. Cancellation is performed serially for multiple AP distributions. Canceling during distribution does not damage the APs. If the distribution on a remote AP is cancelled, the AP will be automatically rebooted. You can cancel distribution to an individual AP at any time except when the status is Updating Flash ... Error, or Done (Rebooting).

If you leave the Software Upgrade panel before the distribution is complete without clicking the **Cancel All**, software distribution continues in the background, but it is not possible to return to the Distribution Status page.

Download Status

During distribution, the Download State column displays the current status of the distribution process (see Figure 187).

Status information is automatically updated every 10 seconds. The status information shows clearly the stage of the distribution process and identifies any problems. Table 17 lists the possible status values and their meaning.

Status	Explanation
Not scheduled	This AP has not been scheduled to receive a software update.
Scheduled	The update has been ordered for this AP, but has not yet begun.
Canceling	A request has been made to cancel the distribution; however, the request is not complete. For example, this message is displayed if a request has been made to cancel distribution to an AP waiting its turn in the distribution list.
Canceled	Distribution to the AP is canceled.
AP Unreachable	The enrolled AP is not reachable for distribution.
Retrying 1, Retrying 2	If communication with the AP is lost during distribution, the process waits for two minutes and then retries the distribution. Three retries are attempted before the process stops and an error message is presented. Retrying 1 and Retrying 2 status represent the first and second retries. Retries may occur, for example, during upgrade of backhaul APs, if the radio signal is temporarily lost and retrunking is required. There is a timeout of two minutes between retries. With a total of three retries, it can take up to 10 minutes before a distribution on an AP is deemed to be in error. The message changes to In Progress .. (XX %) when the retry actually starts.
In Progress .. (XX %)	Upgrade is underway on the AP and is XX% complete.
Error	All retries have finished and the AP could not be upgraded due to some internal error.
Unknown	An unknown error has occurred.
Image Integrity Error	The image has passed the compatibility test but failed the integrity check after the distribution, but before the flash update.
Updating Flashing ...	Image distribution is complete and it is being saved onto the AP's persistent storage.

Status	Explanation
Done. Rebooting	The flashing is complete and the AP is rebooting.

When the distribution is complete, the message Software Distribution is Complete is displayed, regardless of whether the distribution was successful. If a portal AP is not included in the download, all services are restarted automatically after the distribution.

Image Recovery

During the upgrade process, care is taken to validate the image integrity and compatibility with AP hardware. If a new image is successfully upgraded but fails to initialize during subsequent reboot, AP automatically performs a “safe” boot from the backup partition.

Common Problems and Solutions

Table 17 lists common problems that can occur along with recommended solutions.

Table 17: Common Problems and Solutions

Symptom	Problem	Solution
AP power and Ethernet Link LEDs are off	Power is off or unconnected	Check the power connection to make sure it is plugged in. Also check the power outlet. If necessary, plug some other appliance into the outlet to verify power.
AP power LED is on, but the Ethernet Link LED is off	Ethernet cable is unconnected or unable to access the LAN	Check the Ethernet cable connection between the AP and network port. Make sure to use a regular CAT-5 standard Ethernet cable, and not a crossover cable (usually used for uplinks between switches and routers). If in doubt, swap the cable for a known, working cable. If the port is non-functional, it may be necessary to use another working network port.
Unable to configure the Access Point through the web browser interface	Computer is unable to reach the Access Point over the local area network (LAN)	Check to make sure the AP power LED is on. Check the Ethernet cable connections to both the computer and to the AP. Make sure the network adapter in the computer is working properly. Check to see whether the IP address is on the same subnet as the AP. Make sure you are accessing the AP using https:// and not http://.

Table 17: Common Problems and Solutions (continued)

Symptom	Problem	Solution
Poor or lower than expected signal strength, as measured by wireless network adapters attempting to connect to the AP	The AP may be poorly placed, or external antenna may not be connected properly.	The AP and/or its external antenna should not be in an obstructed location. Metallic objects (such as equipment racks) and some construction materials can block wireless signals. If this is the case, reposition the Access Point(s) and/or any external antennae to be free of these obstructions. If using an external antenna, also make sure it is connected securely to the AP.