

encryption provides no protection, and is only recommended when security is not of concern. WPA-AES is recommended for all installations, if possible.

Table 12: Encryption Options

Type	Description
AES	Highest level of protection
TKIP	WEP with additional protection
WEP 128	First generation encryption using 128-bit keys, does not provide adequate protection
WEP 64	First generation encryption using 64-bit keys, does not provide adequate protection
Open	No protection

Configure and view the following aspects of network and user security from the web interface:

- **Wireless Security**—Select protocols for data encryption and user authentication.
- **Authentication Zones**—Group resources for user authentication.
- **Administrator Security**—Set the administrator login and password to access the AP.
- **RADIUS Servers**—Identify authorized RADIUS servers and zones.
- **Security Statistics**—View security-related statistics, including authentication, 802.1x supplicant, and authentication diagnostic statistics.
- **Advanced**—Configured advanced RADIUS properties.

Configuring Wireless Security

Choose **Wireless Security** from the Security Services menu to configure the protocols for data encryption and user authentication. The Wireless Security panel contains two tabs:

- **Security Mode**—Configure WPA, WEP, or open encryption and authentication.
- **SSID Auth**—Identify the authentication server for the SSID.

Security Mode

Use the Security Mode tab (Figure 102) to assign the encryption and authentication methods, including WPA, WEP, or Open. Allowing multiple encryption modes can be useful to support installations with a mixture of client wireless adapters. There are some limitations to the allowed combinations; it is not possible to enable both WEP and Open simultaneously. Also, Open and WPA encryption modes require each mode to be mapped to a separate VLAN (see “Configuring VLANs” on page 105).

Figure 102: Security Services - Security Mode

SECURITY MODE **SSID AUTH** **HELP** **LOGOUT**

Security Services | Wireless Security | Security Modes »

Configure the authentication and encryption policy for your AP.
 You may choose one or more modes from: WPA, WEP, or Open-Access
 * WPA with AES encryption provides the very best security
 * Static WEP-64 keys have to be entered as 10 hex characters
 * Static WEP-128 keys have to be entered as 26 hex characters

Security Configuration

WPA Security Mode

Enable WPA ☒

WPA-EAP ☒ (RADIUS based Automatic Network Keying)
[Configure Auth Server for SSID](#)

WPA Pre-Shared Key ☐ (Manual Key Distribution)
[Configure Key for SSID](#)

Encryption Type aes-only

WEP Security Mode

Enable WEP Based Security ☐

WEP Key-Length 128 - bit

Dynamic WEP with 802.1x ☐ (RADIUS based Automatic Network Keying)
[Configure Auth Server for SSID](#)

Static WEP ☐ (Manual Key Distribution)

WEP Key 1 ☒ Default

WEP Key 2 ☐ Default

WEP Key 3 ☐ Default

WEP Key 4 ☐ Default

Open Access Security Mode (No Encryption)

Enable Open Access ☒

APPLY **RESET**

WPA Security

Select **Enable WPA** to activate the WPA authentication and encryption fields. The following options are available:

Field	Description
WPA Security Mode	WPA-EAP—For RADIUS-based networking keying WPA-PSK—For pre-shared keys
Encryption Type	AES, TKIP, AES and TKIP

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

WPA provides strong encryption support with the AES and TKIP algorithms.



NOTE: Some early versions of WPA-capable client software may not permit a client to associate to the AP when multiple modes off encryption and authentication are chosen.



NOTE: Selecting WPA-EAP or WPA-PSK displays a link that leads to the SSID Authentication tab. Refer to “SSID Authentication” on page 140 for instructions on using this tab.

WEP Security

If it is necessary to configure WEP security, select **Enable WEP** to activate the WEP fields. Configure the following values in the WEP security area:

Field	Description
Enable WEP	Activate the WEP settings. The Airgo AP supports WEP with dynamic and manually entered keys. To use dynamic keys, select WEP, but do not enter values in the Key fields.
Key-Length	Select 64-bit or 128-bit
Key 1 - Key 4	For manual keys, enter up to four WEP key values. Each WEP key is 26 hex-ASCII characters. (required if security mode is WEP)

Click **Apply** to save the settings or **Reset** to clear the fields on the panel.

Open Access

Select **Enable Open Access** to omit data encryption. A pop-up message warns of the potential security risk in using open access. Click **OK** to continue.

SSID Authentication

Use the SSID Authentication tab (Figure 103) to assign RADIUS Authentication servers or a WPA pre-shared key. RADIUS based authentication uses lists of servers, called authentication zones, which are provided by the Airgo AP security portal or an external RADIUS server. Each SSID can be configured with the RADIUS servers used for EAP authentication and the WPA pre-shared key (if applicable).

MAC-ACL lookups can be enabled for clients that associate with WPA-PSK, manual WEP-keys, or with no security. MAC-ACL is not applicable if per user authentication is done where user name is available.

Figure 103: Security Services - SSID Auth

Security Services | Wireless Security | SSID Authentication »

SSID Security Configuration includes:

- * A WPA Preshared Key (if required)
- * Either AP based (Portal) or other (External) RADIUS servers can be configured.
- * MAC address checking can be enabled for this SSID with the security modes: WPA Pre-Shared Key, WEP with manual keys, and Open-Access.

SSID Authentication	
SSID Name *	DeerCreekCo SSID Details
WPA Pre-Shared Key	
Auth Server Configuration	
Security Portal *	☒
	RADIUS Servers: 192.168.168.24
External Auth Servers *	☐ DeerCreekCoAuth
	RADIUS Servers:
Enable MAC Access Control List	☐ (RADIUS based MAC-ACL)
APPLY RESET	

[Configure External Auth Server List](#)

Assign the following values to configure SSID authentication:

Feature	Description
SSID Name	Select from the SSID pull-down list. Click SSID Details to view more SSID-related information, enable multiple SSIDs, or change other SSID attributes.
WPA Pre-Shared Key	Enter the pre-shared key for WPA, if appropriate. This field is grayed out if WPA-PSK is not the selected authentication type.
Authentication Server Configuration	Select the Security Portal or External Authentication Server radio button. For Security Portal, the IP addresses of all security portals are displayed below the radio button. For External security, select from the list of RADIUS servers or click Go at the bottom of the tab to configure the authentication server list (see “Authentication Zones” on page 143). (required)
Enable MAC Access Control List	Select to enable authentication using MAC addresses that are centrally managed in a RADIUS server. For MAC-ACL authentication, it is necessary to use a security portal or external RADIUS server.

Click **Apply** to save changes or **Reset** to return to previously saved values. It may be necessary to click **Back** on your browser to return to the Security Configuration panel. Make sure to also click **Apply** on the Security Configuration panel.

An external RADIUS server can also be added from this tab. Click **Go** at the bottom of the tab to open the Authentication Zone tab of the Authentication Zones panel. For instructions on adding a server, refer to “Configuring Authentication Zones” on page 143.

If an external RADIUS server is to be used for MAC address based ACL lookups, the following apply:

- 1 The RADIUS server must have PAP authentication enabled for these MAC ACL users
- 2 The RADIUS server can expect the AP to send the following standard RADIUS attributes in the authentication request for purposes of policy configuration and interoperability. (MAC addresses must be in sent with no colon or hyphen separators):

Attribute	Description
User-Name	MAC address
User-Password	MAC address
Message-Authenticator	RADIUS extension providing enhanced authentication of message contents. (This is the same as the signature attribute in some RADIUS servers).
NAS-IP-Address	Management IP address of the AP
NAS-Port	Radio interface number for the associating station
NAS-Port-Type	Standard value Wireless - IEEE 802.11. Indicates that the user has requested access via an 802.11 port on the AP.

- 3 The RADIUS server should enforce a policy such that MAC ACL users are only allowed to use PAP authentication for Wireless. This is important because the username and password are not secret.
- 4 The RADIUS server may optionally send back the Session-Timeout attribute to override the AP default session-timeout.
- 5 The RADIUS server may optionally send back an attribute encoded with the user group.

If an external RADIUS server is used for EAP based authentication (with WPA or with legacy 802.1x), the following information should be used when configuring the server:

- 1 The RADIUS server can expect the AP to send the following standard RADIUS attributes in the authentication request for purposes of policy configuration and interoperability:

Attribute	Description
User-Name	Contains the MAC address in the format specified above.
EAP-Message	Contains the EAP messages received from the station.
Framed-MTU	Contains a hint to help the RADIUS server for EAP fragmentation
Message-Authenticator	The RADIUS extension that provides enhanced authentication of the message contents. (Also referred to as signature attribute in some RADIUS servers).
NAS-IP-Address	Contains the management IP address of the AP.
NAS-Port	Contains the radio interface number on which the station is associating.
NAS-Port-Type	Contains the standard value "Wireless - IEEE 802.11" to indicate that the user to be authenticated has requested access via an 802.11 port on the AP.

- 2 The RADIUS server can use these attributes to enforce policies such that EAP based authentication is mandatory for Wireless.
- 3 The RADIUS server may optionally send back the "Session-Timeout" attribute to override the AP default session-timeout.

- 4 The RADIUS server may optionally send back an attribute encoded with the user group.

Configuring Authentication Zones

RADIUS servers may be used to authenticate wireless users and administrative users, and to check MAC Access Control Lists for the SSID.

Select **Authentication Zones** from the Security Services menu to define zones for RADIUS authentication and to add external RADIUS servers to the list of available authentication servers. Configure the servers first, and then include them in zones.

The Authentication Zone panel contains two tabs:

- Auth Zones—Define zones for RADIUS authentication.
- Auth Servers—Add RADIUS servers.

Authentication Zones

On the Authentication Zones tab (Figure 104), you can create new authentication zones or modify existing ones. Select check boxes for authentication zones you want to modify or delete, or click **Add** to add a new zone.

Figure 104: Authentication Zones - Auth Zones

Security Services | Auth Zones | Auth Zone Table »

An 'Auth Zone' is a list of one or more Auth Servers (or RADIUS servers). Each SSID is bound to an Auth Zone. To authenticate a user, identify the Auth Zone that is mapped to that SSID. Then contact each of the Auth Servers in that Auth Zone, until one of them reply to the query. A separate Admin Auth-Zone can be configured to authenticate network administrators.

Auth Zone	Auth Servers	Admin Zone
☐ DeerCreekCoAuth	192.168.168.1	NO

ADD DELETE MODIFY

Set the following values on the Add Auth Zone entry panel (Figure 105):

Field	Description
Auth Zone	Name of the authentication zone.
Auth Server list	List of possible servers to add to the zone. Select desired servers.

Click **Add** after making selections.

Figure 105: Authentication Zones - Add Auth Zones

☐	Auth Server	Port
☐	192.168.168.24	1812
☐	192.168.168.1	1812

To add a new authentication server, click **Add Auth-Server**, and enter the following values for each new RADIUS server:

Field	Description
Auth Server	IP address of the RADIUS authentication server.
Shared Secret	Enter and confirm the secret key.
Port Number	Port number for the server (default is 1812).

Click **Add** to save the values, or click **Reset** to clear the fields on the panel.

Click **Back** on your browser to return to the Auth Zone panel. Set an authentication zone for administrative users by selecting from the pull-down list.

Authentication Servers

Open the Authentication Servers tab (Figure 106) to view the current authentication servers and add or delete servers. This table shows the list of both internal (security portals) and external auth servers. The servers that do not have a check box against them are security portals.

Figure 106: Authentication Zones - Auth Servers

The following lists all Auth Server (RADIUS servers) configured on this AP. A Auth Server is used to authenticate wireless users using WPA or MAC-ACLs. A set of Auth Servers form an Auth Zone. Each Auth Server must be configured with the correct IP address and a shared secret passphrase. The default port number for RADIUS authentication is 1812.

☐	Auth Server	Shared Secret	Port
☐	192.168.168.24	*****	1812
☐	192.168.168.1	*****	1812

Configuring Administrator Security

Choose **Administrator Security** from the Security Services menu to open the Administrator Security panel (Figure 107).

Figure 107: Administrator Security - Admin Password

Set the following values on this panel:

Field	Description
Change Local Admin Password	Enter the old password and the new password, and confirm the new password. This password is used for the local administrative login and the SNMPv3 administrative login. (required)
RADIUS Authentication for Network Administrator Login	Select whether to use the Portal AP security feature for network administrator authentication or use an external RADIUS server. With the external RADIUS server option, links are available to add, delete, or edit the list of servers. (required)

Click **Apply** to save the settings or **Reset** to clear the fields on the panel.

External RADIUS Server Settings

The following rules apply for an external RADIUS server:

- The external RADIUS server must have Password Authentication Procedure (PAP) authentication enabled for administrative users.
- The Airgo AP sends a standard RADIUS attribute called “Service-Type” in the authentication request. The value of this attribute is set to “Administrative” to indicate that the user to be authenticated has requested access to an administrative interface on the AP
- If the user authentication is successful, the RADIUS server must send back an Airgo vendor-specific attribute defined as follows:
`vendor-id=13586, vendor sub-type=3, integer value = 1.`

This attribute informs the AP that the user is not normal user, but rather an administrator who may be granted access to the privileged administrative interface.

Viewing Security Statistics

Choose **Security Statistics** item from the menu tree to open the Security Statistics panels. This panel contains the following tabs:

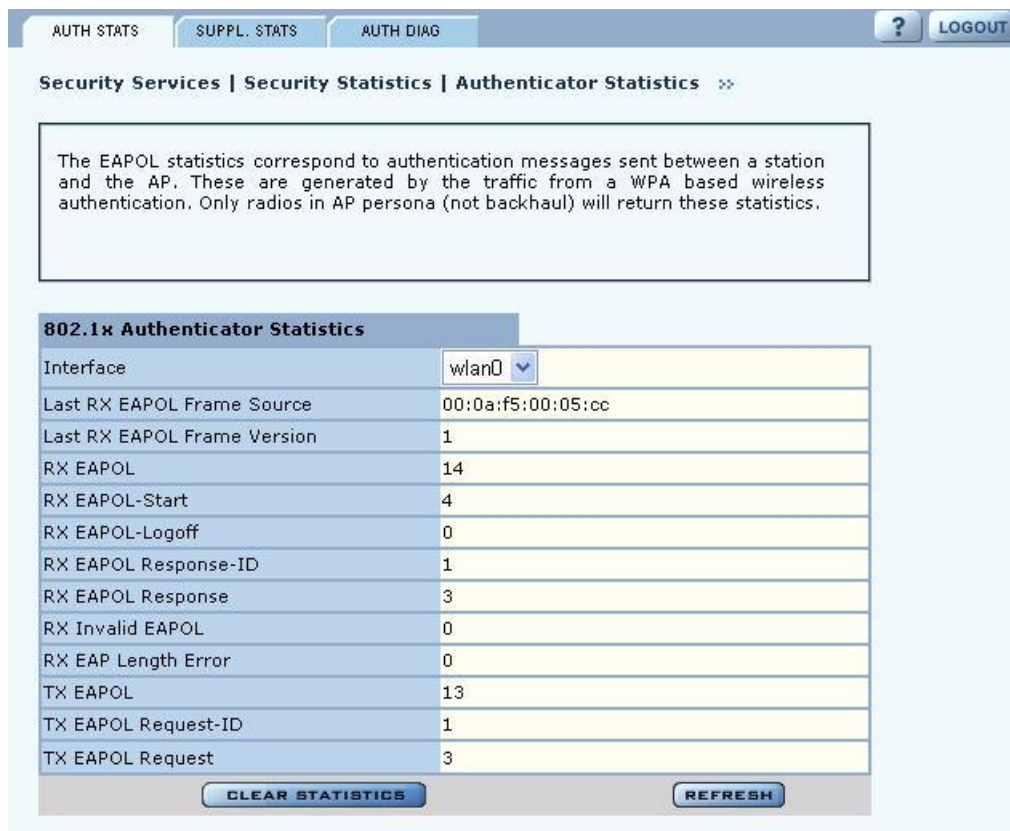
- Auth Stats—View authentication statistics for each selected AP radio.
- Suppl Stats (Supplicant Statistics)—View statistics on 802.1x requests, for each selected BP radio.
- Auth Diag—View authentication diagnostics statistics, including back-end data.

Each of the tabs includes a Reset button to return the statistics to zero and begin collecting them again.

Authentication Statistics

The Authentication Statistics tab (Figure 108) contains EAPOL statistics, which correspond to authentication messages sent between a station and an AP. These are generated by the traffic from WPA or 802.1x based wireless authentication. Only radios in AP mode produce this data.

Figure 108: Security Statistics - Authentication Stats



The tab contains the following information:

Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the AP. This identifies a station or BP that is currently authenticating or re-authenticating with the AP.
Last RX EAPOL Frame Version	The EAPOL version from the last EAPOL frame received by the AP.
RX EAPOL	The total number of EAPOL frames received by the AP.
RX EAPOL-Start	The total number of EAPOL-Start frames received by the AP. This count increments as stations or BPs request the AP to start their authentication sequence.
RX EAPOL-Logoff	The total number of EAPOL-Logoff frames received by the AP. This count may not increment as most 802.1x peers do not send this frame for security reasons.
RX EAPOL Response-ID	The total number of EAPOL based EAP Response-ID frames received by the AP. This count increments as stations or BPs present their user-id or device-id information to the AP at the start of the authentication sequence.
RX EAPOL Response	The total number of EAPOL based EAP Response frames received by the AP that do not contain an EAP Response-ID. This count increments as the AP receives authentication credentials derived from passwords or certificates from stations or BPs that are authenticating with it.
RX Invalid EAPOL	The total number of EAPOL frames received by the AP that have invalid packet type fields. These frames are discarded by the AP.
RX EAP Length Error	The total number of EAPOL frames received by the AP that have invalid packet body length fields. These frames are discarded by the AP.
TX EAPOL	The total number of EAPOL frames transmitted by this AP.
TX EAPOL Request-ID	The total number of EAPOL based EAP Request-ID frames transmitted by this AP. This count increments as the AP sends authentication frames to stations or BPs requesting them to return their user-id or device-id information at the very start of the authentication sequence.
TX EAPOL Request	The total number of EAPOL based EAP Request frames transmitted by the AP that do not contain an EAP Request-ID. This count increments as the AP transmits authentication credentials derived from passwords or certificates to the stations or BPs that are authenticating with it.

Supplicant Statistics

The Supplicant Stats tab(Figure 109) reports on authentication messages sent between a local BP radio and the upstream AP. Only radios in BP mode return these statistics. The statistics are generated from the EAPOL protocol, which is used for 802.1x authentication.

Figure 109: Security Statistics - Supplicant Stats

Security Services | Security Statistics | Supplicant Statistics »

The EAPOL statistics correspond to authentication messages sent between a local BP radio and the upstream AP. Only radios in BP persona will return these statistics.

802.1x Supplicant Statistics

Interface	wlan0
Last RX EAPOL Frame Source	Not Applicable
Last RX EAPOL Frame Version	Not Applicable
RX EAPOL	Not Applicable
RX EAPOL Request-ID	Not Applicable
RX EAPOL Request	Not Applicable
RX Invalid EAPOL	Not Applicable
RX EAP Length Error	Not Applicable
TX EAPOL	Not Applicable
TX EAPOL-Start	Not Applicable
TX EAPOL-Logoff	Not Applicable
TX EAPOL Response-ID	Not Applicable
TX EAPOL Response	Not Applicable

CLEAR STATISTICS **REFRESH**

The tab contains the following information:

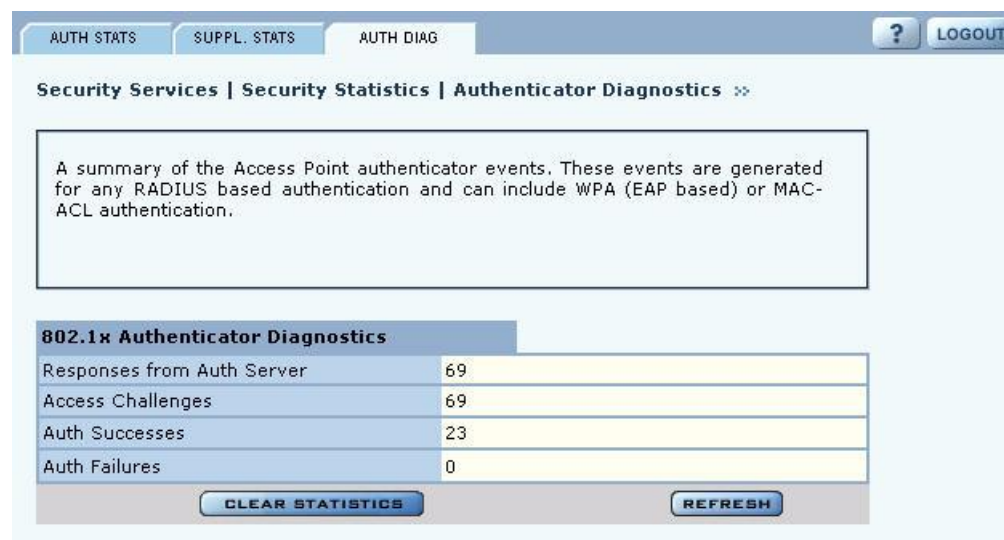
Field	Description
Interface	Select the radio interface of interest for viewing statistics.
Last RX EAPOL Frame Source	The source MAC address from the last EAPOL frame received by the BP. This identifies the upstream AP that is currently authenticating or re-authenticating with the BP.
Last RX EAPOL Frame Version	The EAPOL version from the last EAPOL frame received by the BP.
RX EAPOL	The total number of EAPOL frames received by the BP.
RX EAPOL Request-ID	The total number of EAPOL based EAP Request-ID frames received by this BP. This count increments as the AP sends authentication frames to the BP requesting it to its device-id information at the very start of the authentication sequence.
RX EAPOL Request	The total number of EAPOL based EAP Request frames received by the BP that do not contain an EAP Request-ID. This count increments as the AP transmits authentication credentials derived from certificates to the BP.
RX Invalid EAPOL	The total number of EAPOL frames received by the BP that have invalid packet type fields. These frames are discarded by the BP.
RX EAP Length Error	The total number of EAPOL frames received by the BP that have invalid packet body length fields. These frames are discarded by the BP.

Field	Description
TX EAPOL	The total number of EAPOL frames transmitted by this BP.
TX EAPOL-Start	The total number of EAPOL-Start frames transmitted by the BP. This count goes up as the BP requests the AP to start its authentication sequence.
TX EAPOL-Logoff	The total number of EAPOL-Logoff frames transmitted by the BP. This count will not increment as the BP does not send this 8021.x frame for security reasons.
TX EAPOL Response-ID	The total number of EAPOL based EAP Response-ID frames transmitted by this BP. This count increments as the BP sends authentication frames to the AP with its device-id information at the very start of the authentication sequence.
TX EAPOL Response	The total number of EAPOL based EAP Response frames transmitted by the BP that do not contain an EAP Response-ID. This count increments as the BP transmits authentication credentials derived certificates to the AP that is authenticating with it.

Authentication Diagnostics

The Authentication Diagnostics tab (Figure 110) contains a summary of the Access Point authenticator events received from a backend authentication server. These events are generated for any RADIUS based authentication and can include WPA (EAP based) or MAC-ACL authentication.

Figure 110: Security Statistics - Authentication Diagnostics



The tab contains the following information:

Field	Description
Responses from Auth Server	The total number of RADIUS authentication related packets received from the backend authentication server.
Access Challenges	The total number of RADIUS authentication packets that contained an ACCESS-CHALLENGE. These are sent by the RADIUS server when it is engaged in a multi-step authentication sequence.

Field	Description
Auth Successes	The total number of RADIUS authentication packets that contained an ACCESS-ACCEPT. These are sent by the RADIUS server when the authentication sequence succeeds.
Auth Failures	The total number of RADIUS authentication packets that contained an ACCESS-REJECT. These are sent by the RADIUS server when the authentication sequence fails.

Configuring Advanced Parameters

Choose **Advanced Configuration** from the menu tree to open the Advanced RADIUS configuration panel (Figure 111). It is not necessary to modify any of the settings on this panel.

Figure 111: Advanced Configuration - Timeouts

TIMEOUTS HELP LOGOUT

Security Services | Advanced Configuration | Timeouts & Misc. >>

It is recommended to use defaults for these Security setting. Changing Session Time and Group Key Interval changes time when WPA group key expires. Change RADIUS timeout and retries if there is network latency to reach RADIUS server(s) (e.g., over a WAN link). Configure a RADIUS attribute that can map to user-group attribute to select service-profiles.

Timeouts

Session Timeout (in seconds)	28800
Group Key Interval (in seconds)	3600
RADIUS Timeout (in seconds)	3
RADIUS Retries	2

RADIUS Attribute for User-Groups

RADIUS Standard Attribute	☐
Attribute Type	
Vendor-Specific Attribute	☒
Vendor ID	13586
Vendor Sub-type	1
Interpretation	☒ String ☐ Integer

APPLY RESET

The panel contains the following fields:

Field	Description
Session Timeout	Time in seconds, after which a station is re-authenticated
Group Key Interval	Time in seconds, after which the group key is changed. This is not used if static WEP keys are enforced
RADIUS Timeout	Time in seconds, after which the request is retransmitted

Field	Description
RADIUS Retries	Number of retransmit attempts, after which the RADIUS request is marked a failure.
External RADIUS Group-Key Attribute (for User Group ID)	RADIUS attribute used by the AP to determine the user group (see “SSID Details” on page 82). When a wireless user is authenticated by a RADIUS server, the server can optionally send the AP the ‘User Group’ for the association. If a user group is not returned, then the user is not assigned a group, and the user gets the default service profile for the SSID. By default, a Vendor Specific Attribute is used (13586, 1, String).

Other standard or vendor specific attributes can be used to determine service policies. For example, an enterprise having an existing RADIUS attribute for VLANs can reuse the attributes for AP service profile assignments by configuring them as the RADIUS attributes for user groups.

Click **Apply** to implement the changes, or click **Reset** to return the entries on the panel to their previous values.

8 Configuring Guest Access

This chapter describes how to enable guest user access to the wireless network while protecting the network from unauthorized use. It contains the following sections:

- [Overview](#)
- [Configuring Guest Access](#)
- [Guest Access Services Panel](#)

Overview

Guest access can be used to allow visitors to a facility to access the Internet through the wireless network without gaining access to the corporate network. Most current guest user solutions require guests to access a separate access point that is not part of the corporate network. The Airgo solution eliminates this requirement by restricting guest access through VLAN tags on the existing access points. There is no need to set up special access points or to physically restrict the locations used for guest access.

Unauthenticated users are permitted to associate to an AP, but any web communications are captured and directed to a controlled landing page, the “captive portal.” The landing page allows the guest user to login using a web-based password scheme. The page can inform unauthenticated users of the network access policies and provide instructions on obtaining the guest password. Following successful authentication, the guest user is released from the captive pages and allowed to access any resource on the guest VLAN.

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.

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.

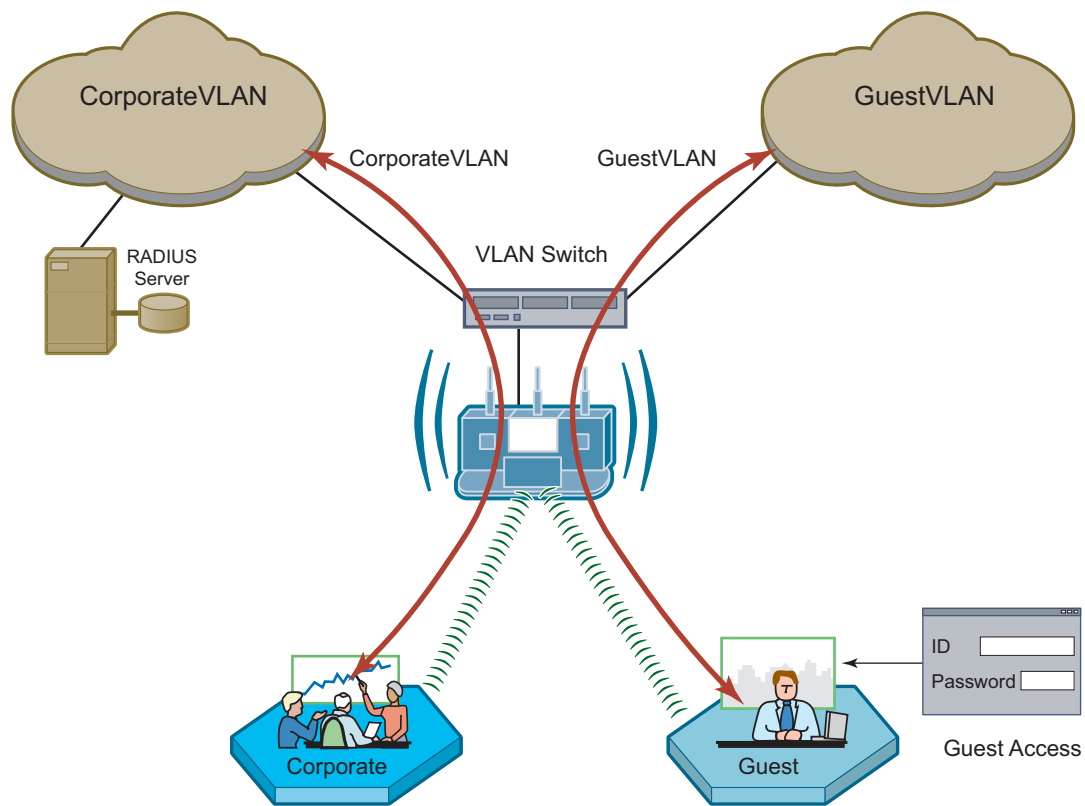
Guest user authentication can be implemented using an internal or external landing page.

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 Airgo security portal. If either password is acceptable, the guest user is authenticated and receives the privileges specified in the guest service profile.

Figure 112 shows how Acme Works configured guest access with an internal guest landing page. 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 112: Guest Access - Internal Landing Page



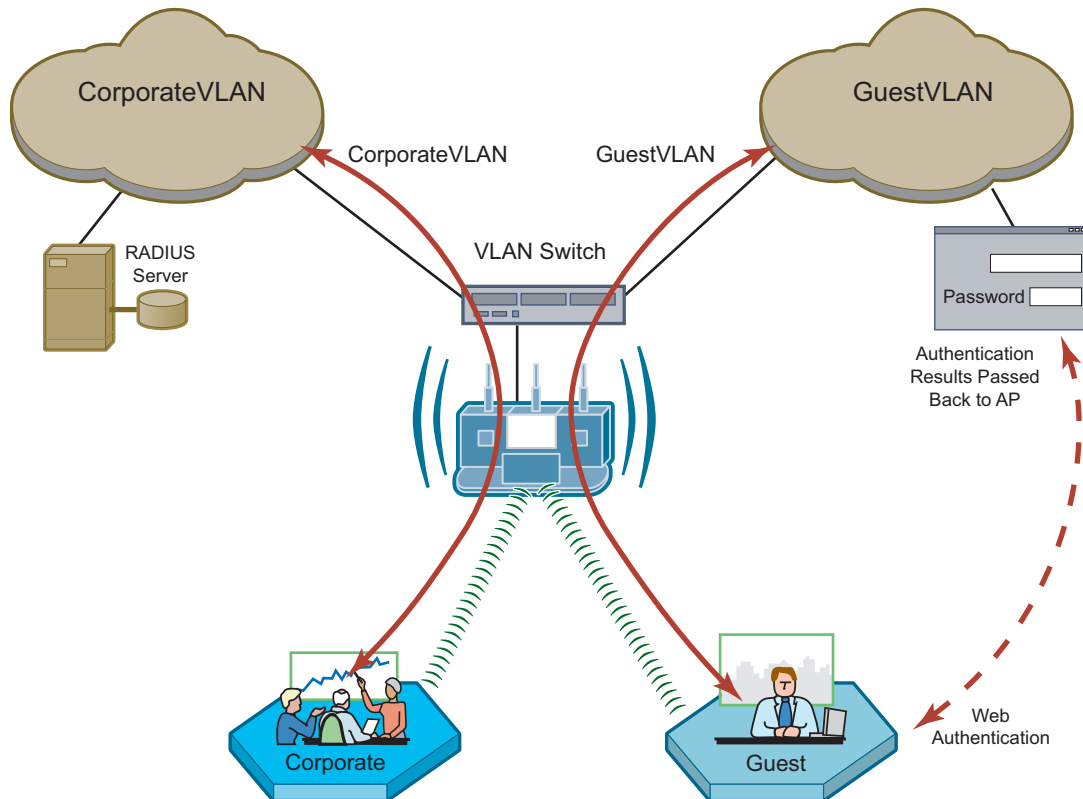
A0045B

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

Figure 113 shows a network 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 113: Guest Access - External Landing Page



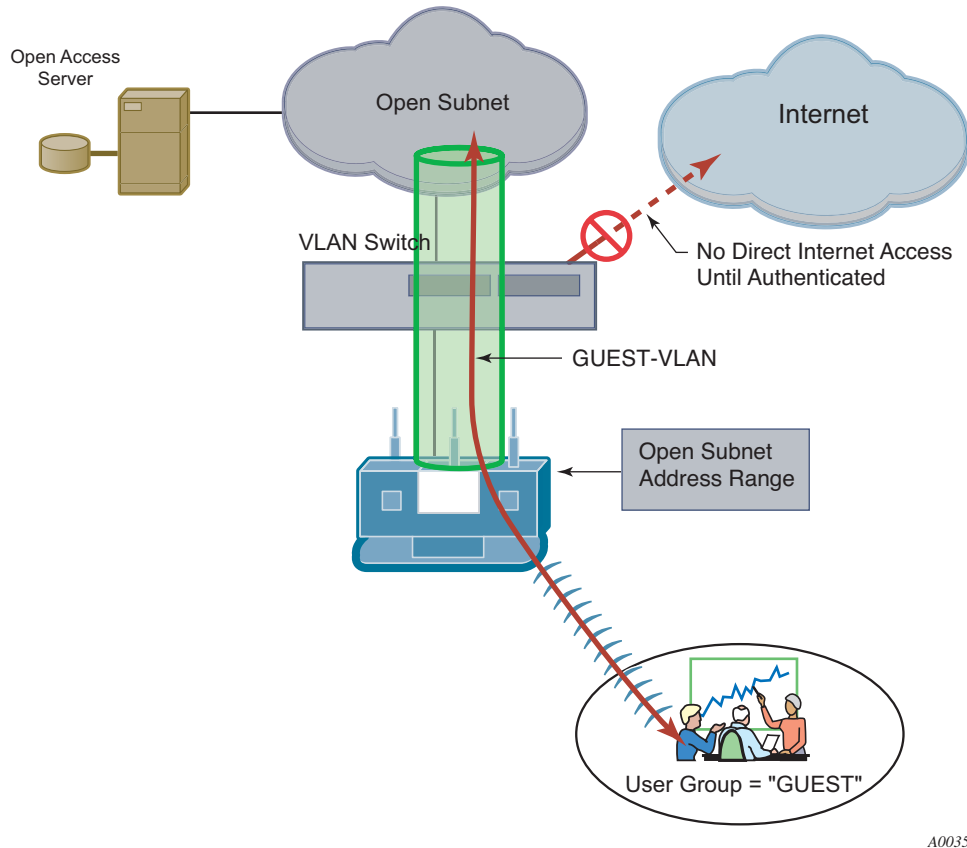
A0045B

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

Open Subnet

In an optional open subnet arrangement, shown in Figure 114, 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 114: Guest Access - Open Subnet



Configuring Guest Access

This section describes the complete process of setting up guest access. A Guest Access wizard is also available for easy configuration of the major guest access parameters. See “Guest Access Wizard” on page 50 for instructions on using the Guest Access wizard.

Task

Confirm that open access is supported as a security option.

Steps

- 1 Choose **Wireless Security** from the **Security Services** menu to open the Security Mode tab (“Configuring Wireless Security” on page 138).
- 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**.

Task (continued)	Steps
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 106). 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 106). 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 to 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 105.
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 79). 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.
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 82). 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.

Task (continued)	Steps
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 then 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 117), 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.

Guest Access Services Panel

For summary information about guest access, use the Guest Access Configuration panel. The panel opens to the Guest table (Figure 115), which lists currently defined guest service profiles. The 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 displayed 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 115: 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.

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. 2 Select 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 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.

Function	Description
Delete an entry	6 Select the entry and click Delete . 7 Click OK to confirm.

Guest Access Security

The Security tab of the Guest Access Configuration panel (Figure 116) provides an interface to set the guest password for an internal landing page.

Figure 116: 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 117).

Figure 117: 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	Daily
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](#)
- [Managing Users](#)

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.

Airgo offers the unique advantage of a network management capability 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 to mid-size networks, this eliminates the need for an external network management application. For mid to large size enterprise networks, NM Portal can be used to 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

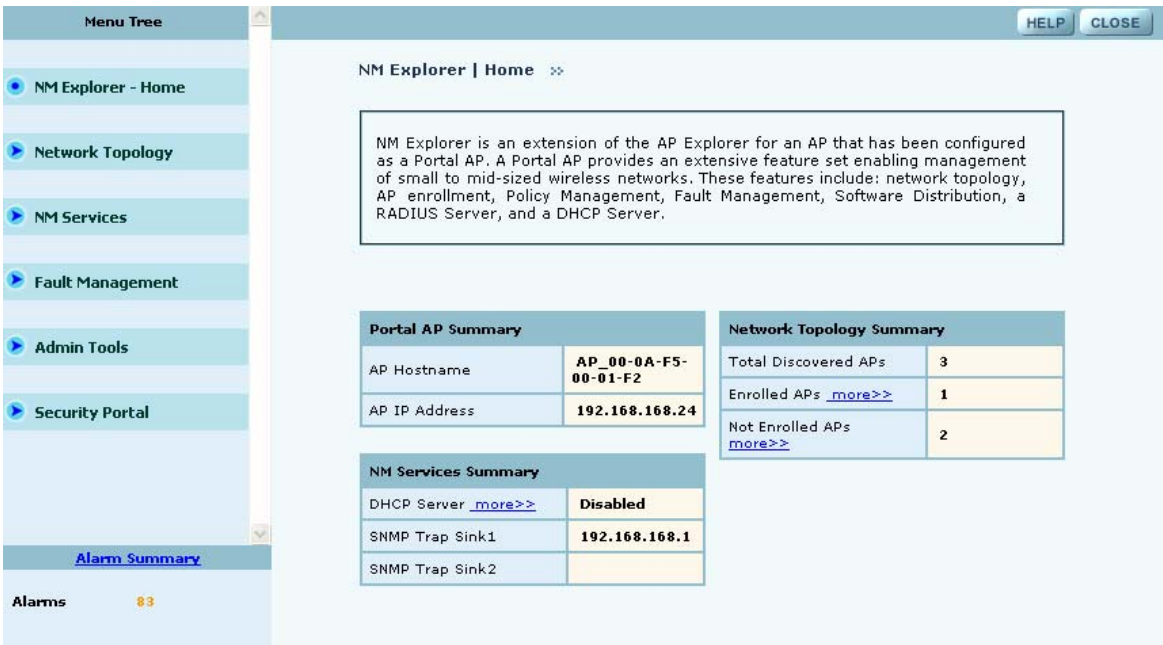
Using NM Portal

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,” 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 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 37). The NM Portal Network Management Explorer opens in a new browser window (Figure 118).

Figure 118: 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 to access 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 NM Portal managed network.

Home Panel

The Home panel (Figure 118) 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, and radio neighbors.
- NM Services—Set up 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 219).
- Security Portal—Add network, administrative, and legacy users.

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

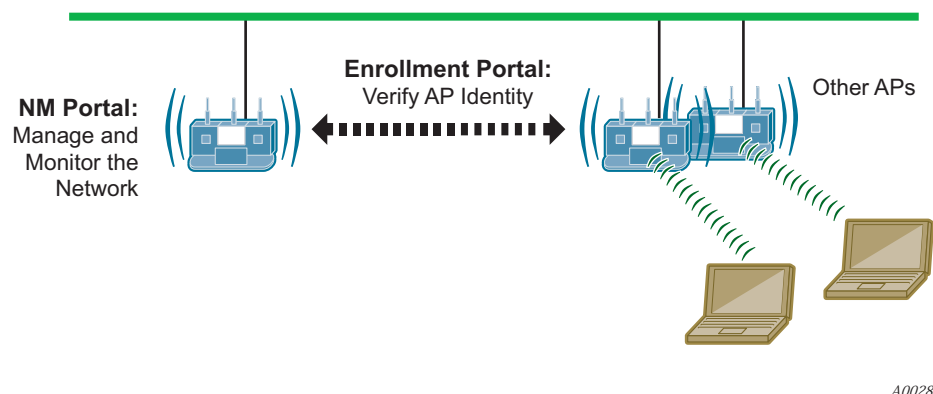
Network security depends upon mutual trust between the NM Portal and the other managed Airgo APs. Each access point must trust the identity of the NM Portal AP, and the NM Portal must trust that each access point is fully authenticated (Figure 119). Enrollment is the process used to establish this mutual trust. The process consists of several steps:

- NM Portal automatically discovers all the Airgo Access Points and presents those that are 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.

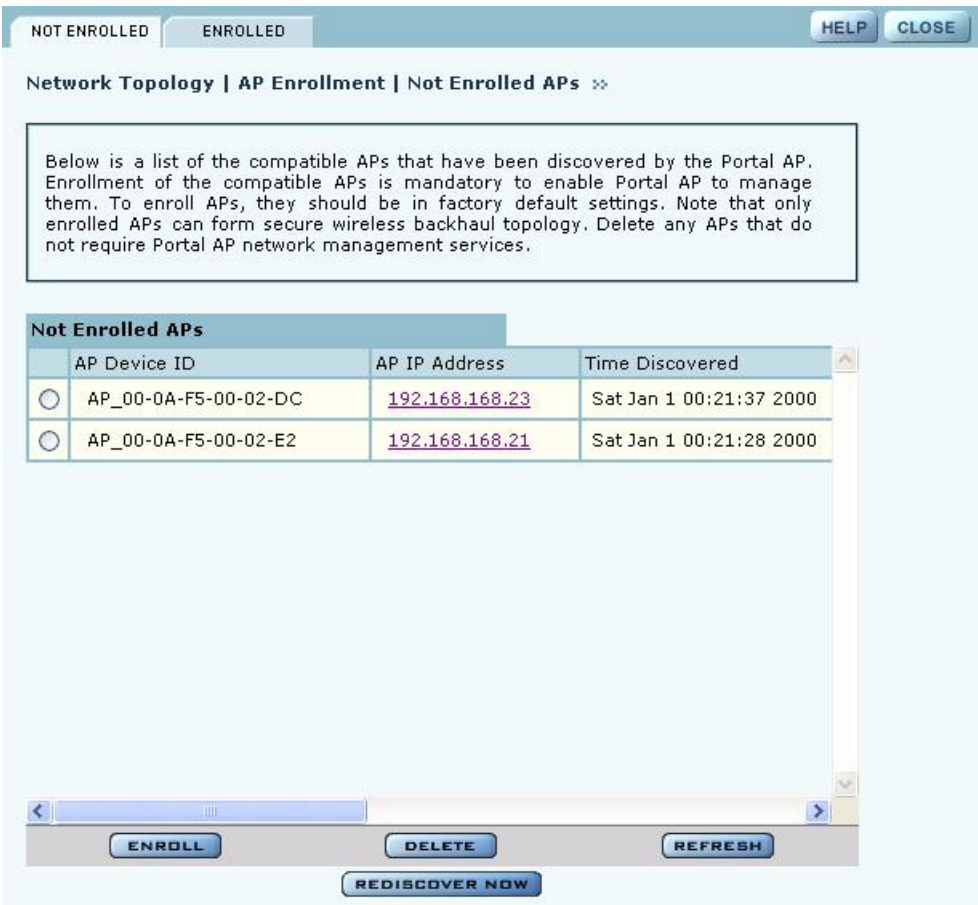
An NM Portal can discover up to 50 APs across multiple IP subnets, but can only enroll up to 20 APs. To access the enrollment panel, choose **AP Enrollment** from the Network Topology menu. The AP Enrollment panel opens to display the list of discovered, but as yet un-enrolled, APs (Figure 120).

Figure 119: AP Enrollment



A0028A

Figure 120: 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 121). 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 13), 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.
Refresh	Click to update the display.
Rediscover Now	Scan the network to discover APs and update the Not Enrolled APs table.

Figure 121: Network Topology - AP Enrollment - Enroll an AP Entry Panel

Enroll an AP	
AP Device ID	AP_00-0A-F5-00-01-89
IP Address	192.168.88.101
Serial Number	AIRGO-P2-0xxxxxxxxx
Verify AP ThumbPrint	f2:1a:bd:e3:c7:86:1a:65:81:f4:dc:ca:cb:ad:01:59:af:79:5a:3b
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 13: AP Enrollment Information

Field	Description
AP Name	Verify the alphanumeric name of the AP. The default is the IP address.
IP Address	Verify 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 Airgo-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," for bootstrap configuration details.

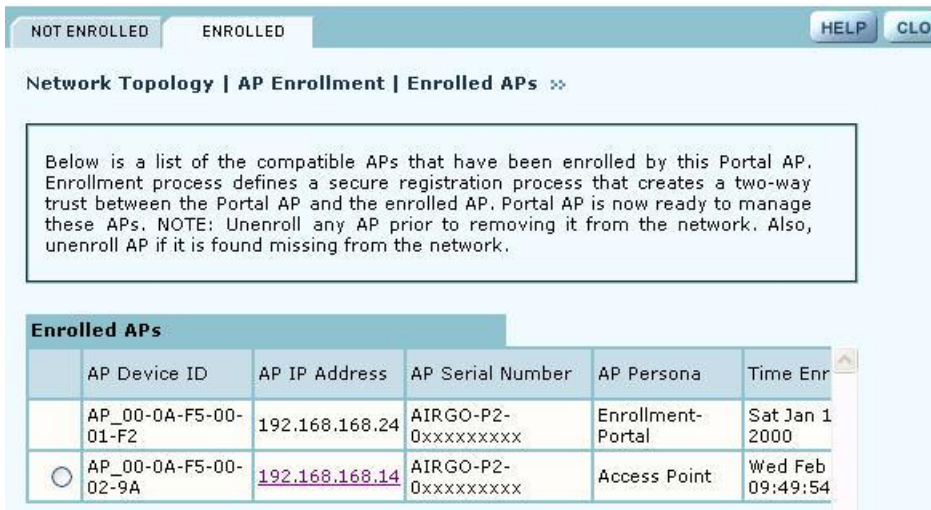
Enrolled APs

Enrolled APs are listed on the Enrolled tab of the Enrollment panel (Figure 122). 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, there is no interruption to service, and all security credentials remain intact.

Figure 122: Network Topology - AP Enrollment - Enrolled



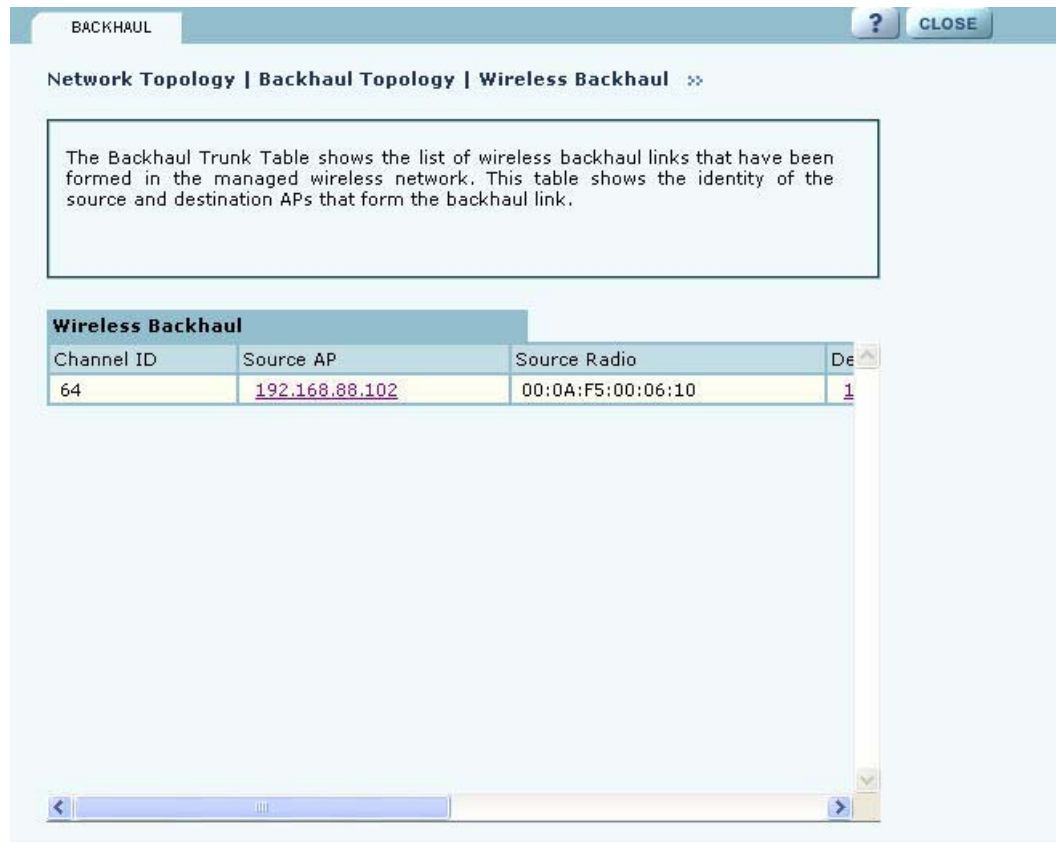
Perform the following functions as needed from the Enrolled APs tab:

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 123).

Figure 123: 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 uplink 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	MAC address of the radio that ends the backhaul trunk
Destination Radio	Radio used for the destination (wlan0 or wlan1)
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 (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	Begins the rediscovery process.

Viewing IP Topology

The IP Topology panel lists all the APs discovered by NM Portal. Choose **IP Topology** from the Network Topology menu to display this information (Figure 124).

Figure 124: Network Topology - IP Topology

The screenshot shows a web interface titled "IP TOPOLOGY" with "HELP" and "CLOSE" buttons. Below the title bar, there are tabs for "Network Topology", "IP Topology", and "Discovered APs". A text box explains that the list below shows compatible APs discovered by Portal AP, and that the discovery service runs periodically. It advises pressing the "Rediscover Now" button if a newly installed AP is not found. Below this is a table titled "IP Discovered APs" with columns: Name, Device Id, Operation State, MAC Address, and Auto/Manual. The table lists three APs with their respective IP addresses, device IDs, operation states, and MAC addresses. At the bottom of the window, there are "DELETE" and "REDISCOVER NOW" buttons.

Below is a list of compatible APs that have been automatically discovered by Portal AP. By default the IP subnet of Portal AP is used to discover these APs. Since discovery service runs periodically, if the newly installed AP is not found on this list, press the Rediscover Now button and refresh this screen in a few minutes.

	Name	Device Id	Operation State	MAC Address	Auto/Manual
☒	192.168.168.24	AP_00-0A-F5-00-01-F2	enable	00:0A:F5:00:06:5A, 00:0A:F5:00:06:17	auto-discovered
☐	192.168.168.23	AP_00-0A-F5-00-02-DC	enable	00:0A:F5:00:06:B4, 00:0A:F5:00:06:B0	auto-discovered
☐	192.168.168.21	AP_00-0A-F5-00-02-E2	enable	00:0A:F5:00:06:DC, 00:0A:F5:00:06:35	auto-discovered

DELETE

REDISCOVER NOW

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 5 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: • 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 a 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, since 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 from one managed network to another.

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 125), accessible from the Discovered Radios item under Network Topology menu in the menu tree.

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

Figure 125: 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 which 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 (they are reachable by way of IP addressing).
Signal Strength	Strength of the detected signal as a percentage
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

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 182.

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 Discover Configuration panel (see “Configuring Network Discovery” on page 182). 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 165. A variety of conditions may cause NM Portal to label an AP as a rogue candidate:

- The AP is in a subnet not included in the discovery domain.
- 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.

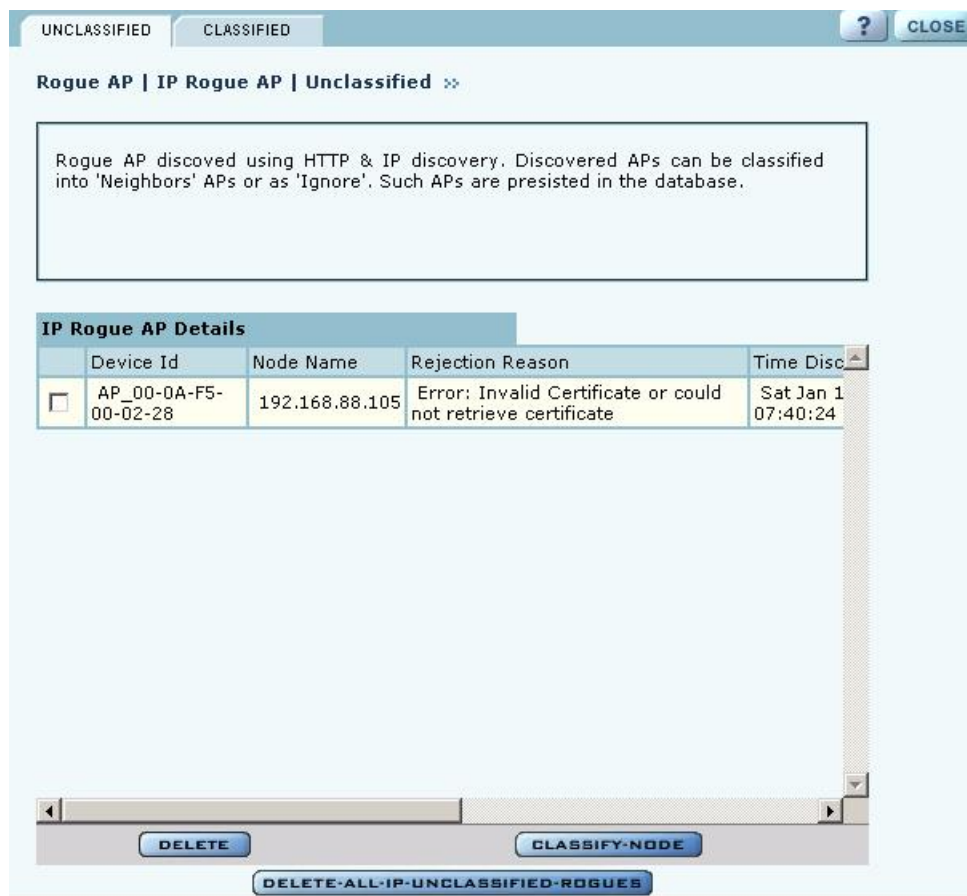
Each panel opens to the Unclassified tab, which lists the candidate rogue APs. From the list, select individual APs to classify as known in your network or a neighbor’s network. Once classified, the APs are listed in the IP or Wireless Classified tab.

IP Rogue AP Management

Select IP Rogue AP from the Rogue AP menu to open the table of IP-unclassified APs. This panel (Figure 126) 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. This value is updated each time the AP is detected.
Thumbprint	Factory-generated identifier used for AP enrollment

Figure 126: 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 Airgo device ID and IP address, if known. 2 Click Classify-Node to open the Classify the Rogue AP panel (Figure 127). 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 128). 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 127: IP Rogue AP - Classify

Classify the Rogue AP

Rogue AP IP Address: 192.168.88.102

Rogue AP MAC Address:

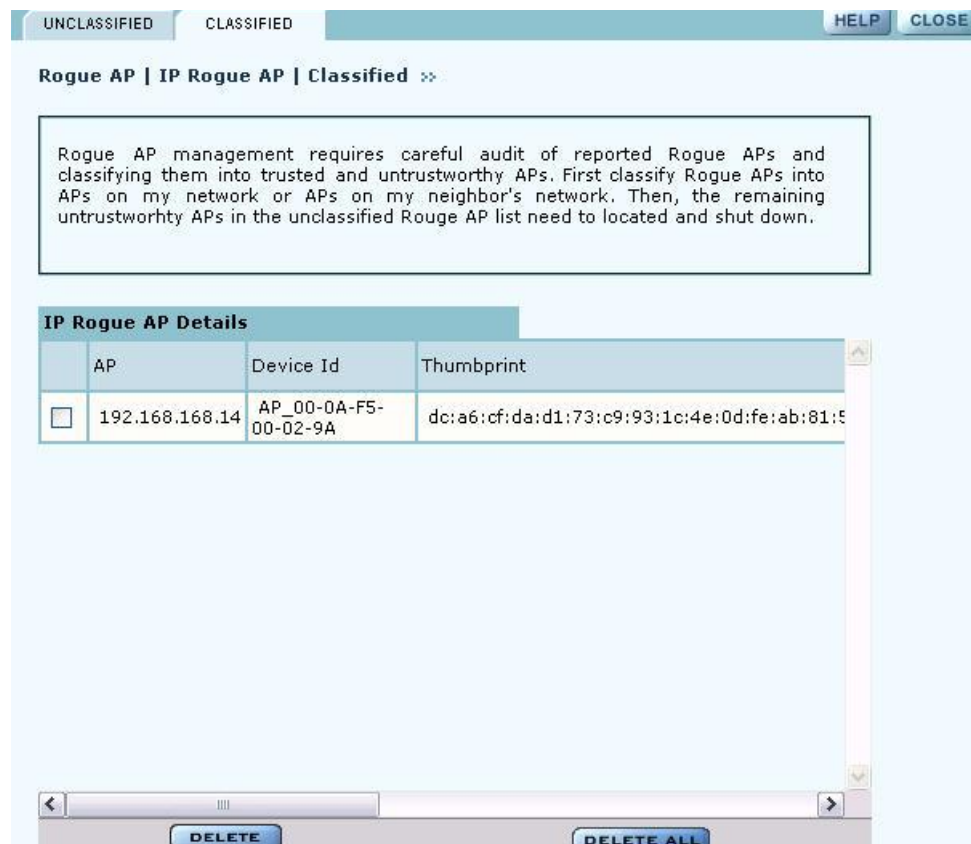
Rogue AP Class: ☒ Our-Network ☐ Neighbor-Network

APPLY **RESET**

Classified Tab

The Classified tab (Figure 128) 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. This value is 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 128: IP Rogue AP - Classified

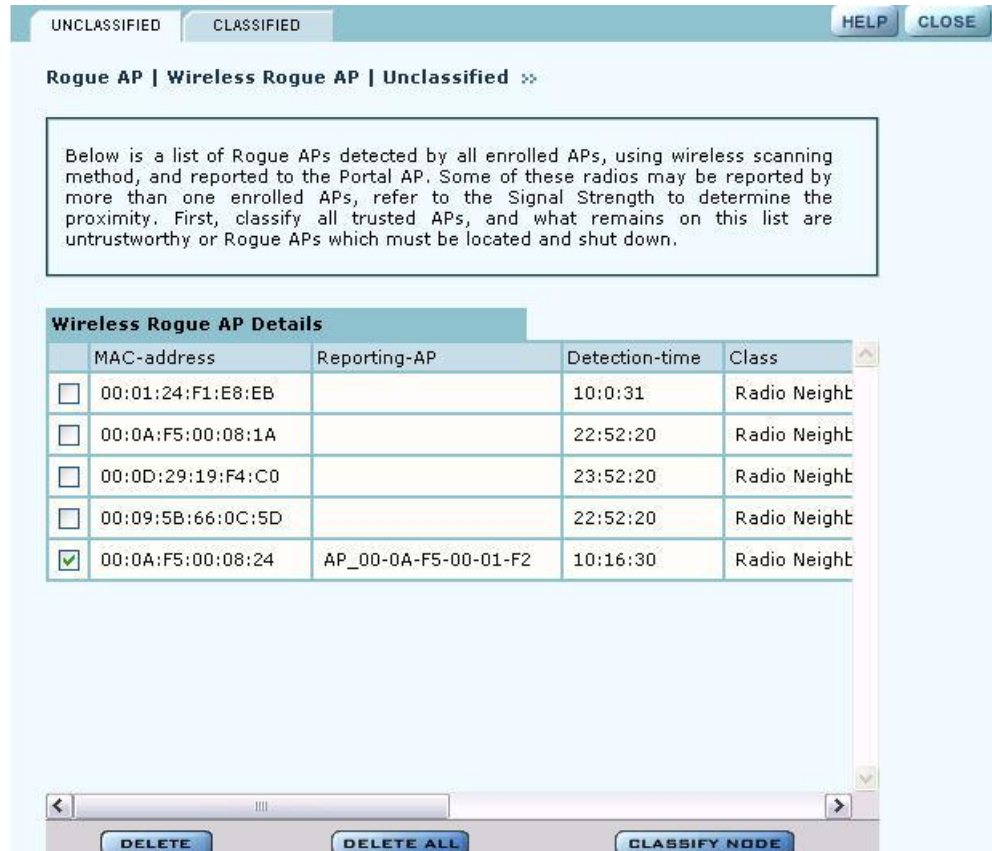
Wireless Rogue AP Management

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 129) lists the following information for each IP rogue:

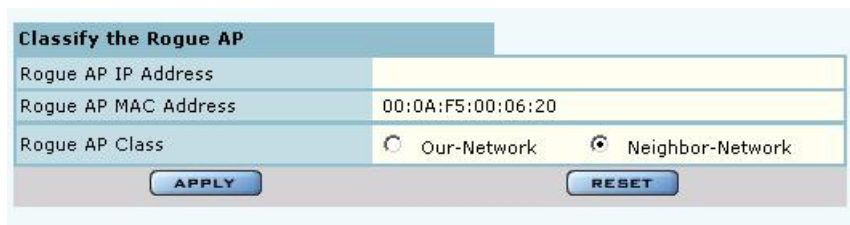
Field	Description
MAC Address	MAC address of the unclassified rogue AP
Reporting AP	The device ID of the AP or APs that identified the rogue AP. If this field is empty, that means that the rogue device was detected in a previous scan, but not in the most recent scan.
Detection Time	Time that the AP was last detected
Class	Radio Neighbor or Radio & 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 129: 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 130). 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 131). 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 130: Wireless Rogue AP - Classify


Classify the Rogue AP

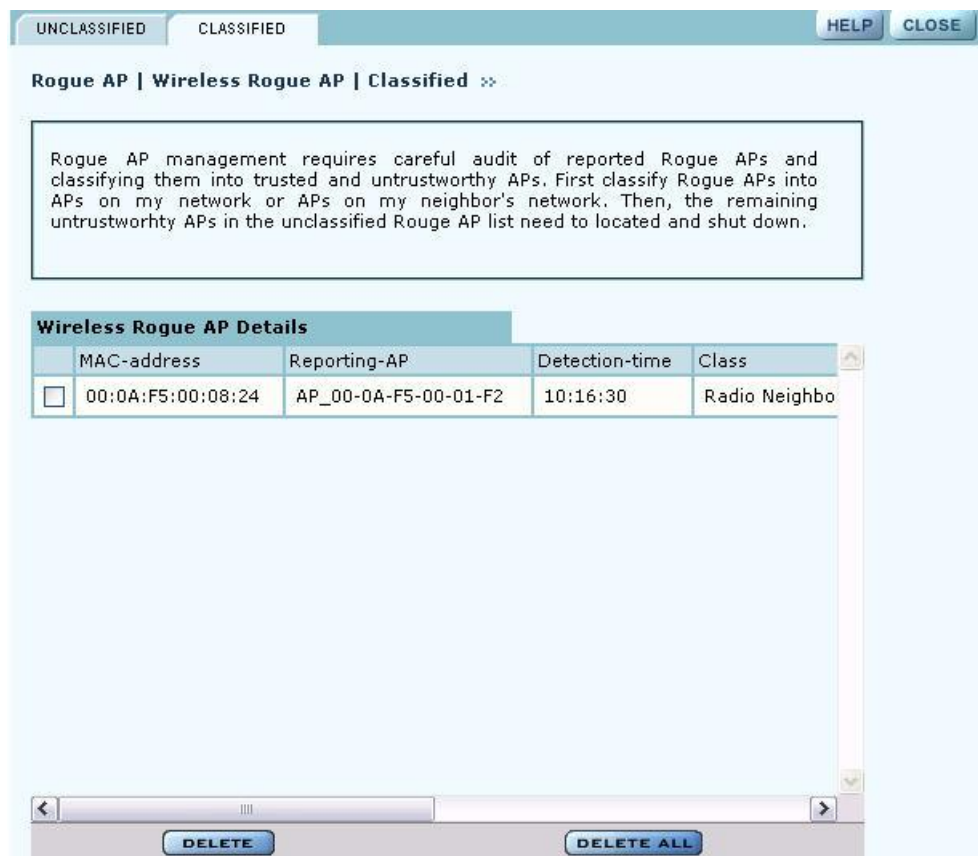
Rogue AP IP Address	
Rogue AP MAC Address	00:0A:F5:00:06:20
Rogue AP Class	☐ Our-Network ☒ Neighbor-Network

APPLY RESET

Classified Tab

The Classified tab (Figure 131) 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	IP address of the AP that reported the detected AP
Detection Time	Time of the scan that last detected the AP
Class	Category used to classify the AP

Figure 131: 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

DELETE DELETE ALL

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

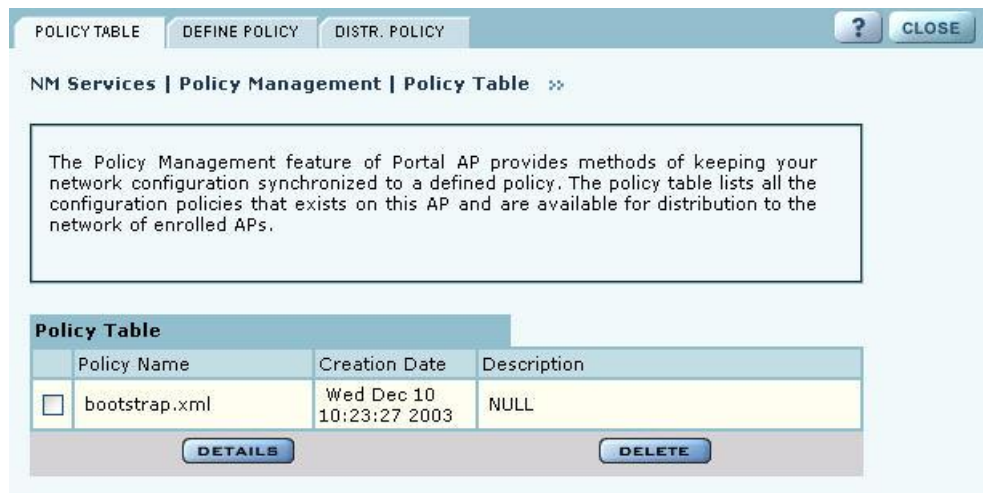
Policy Management provides tools to keep your network configuration synchronized to a defined set of rules. Open the Policy Management panel to manage configuration policies for distribution to the network of enrolled APs. The panel contains the following tabs:

- 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 132) lists policies that exist on this AP and are available for distribution to the network of enrolled APs.

Figure 132: 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 132). To return to the policy table, click **Back**. To delete a policy, click **Delete**.

Figure 133: 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 134) to choose the default policy.

NOTE: The Portal AP requires two radios in order to construct a default policy for 2-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 134: NM Services - Policy Management - Define Policy

The screenshot shows the 'Define Policy' tab selected in the 'NM Services | Policy Management' menu. The interface includes a 'POLICY TABLE' tab, a 'DEFINE POLICY' tab (active), and a 'DISTR. POLICY' tab. A 'HELP' button and a 'CLOSE' button are in the top right. A text box explains: '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 'Generate Default Policy' section 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 135) to direct how policies are shared across the network.

Figure 135: NM Services - Policy Management - Distribute Policy

The screenshot shows the 'Distribute Policy' tab selected in the 'NM Services | Policy Management' menu. The interface includes a 'POLICY TABLE' tab, a 'DEFINE POLICY' tab, and a 'DISTR. POLICY' tab (active). A 'HELP' button and a 'CLOSE' button are in the top right. A text box explains: '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 'Distribute Policy' section with a 'Select Policy To Distribute' dropdown menu showing 'defaultpolicy.xml'. There is a 'Select All Policies To Distribute' checkbox which is unchecked. Below this is a table with a 'Target AP Name' column and three rows of IP addresses: 192.168.88.101, 192.168.74.241, and 192.168.74.203. Each row has an unchecked checkbox. 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 136).

Figure 136: NM Services - Discovery 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

Manually Add an AP to Topology DB

AP IP Address

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).

Field	Description
Discovery Limit	Restrict discovery to a number of APs. Once this limit is reached, the discover process stops. The range is 1-50 for (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. AP's added to the managed network this way are termed “manually added” and can be managed by NM Portal. This option is useful if an AP is moved to another subnet and is no longer able to reach the NM Portal AP. You can manually add the AP’s IP address in NM Portal and continue manage the AP. It is not necessary to reenroll the AP.
Discovery Methods	Select whether to discover the APs with valid IP address information (IP), 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 **Discover** 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 136) to configure the scope and seed parameters.

Figure 137: 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	192.168.168.20
Discovery Scope - Subnet Maskbits	255.255.255.0
Discovery Seed - AP IP Address	192.168.168.24

APPLY RESET

Discovery Scope Table

☐ Discovery Scope IP Subnet	Discovery Seed AP IP Address
☐ 192.168.168.1/24	192.168.168.24

DELETE

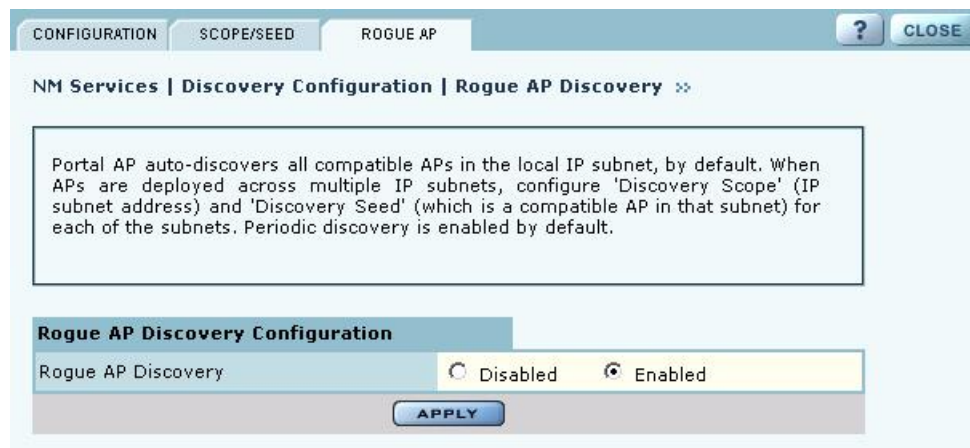
Configure the following fields on this tab:

Field	Description
Discovery Scope	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.

Rogue AP

Use the Rogue AP tab (Figure 136) 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 173.

Figure 138: 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 139) to manage the security portals for the network.

Figure 139: 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 . 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 using which the portal may be deleted.

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 synchronized with the NM Portal database. Click Apply to save the settings, or click Reset to return to the default values (autonomous selected, period 5 minutes). It is recommended to accept the default value to make sure that synchronization takes place.
Portal DB Version Table	View current database information for user security. For each AP designated as a security portal, 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 139) to save the NM Portal database and configuration using the secure https protocol.

Figure 140: 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 [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 on the AP disk, so it is recommended to 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 141) to back up the portal databases and configuration to a TFTP server and to restore the configuration from the TFTP server. For backup and restore, enter the server IP address and specify a backup file name. For 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 141: 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 four 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



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

DHCP Options

Select the DHCP Options tab (Figure 142) to activate and configure the DHCP server.

Figure 142: NM Services - DHCP Configuration - DHCP Options

DHCP OPTIONS | IP RANGE | LEASES | STATIC IP | **HELP** | **CLOSE**

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
Maximum Leases	Specify the maximum number of available leases. There is no default.
Gateway	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 143).

Figure 143: NM Services - DHCP Configuration - IP 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

Interface Name:

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
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 Address/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 144) lists each network computer serviced by DHCP and its lease information.

Figure 144: 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 145) to reserve static IP addresses for specific nodes.

Figure 145: 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
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 146) provides an aggregate count of alarms across the network managed by NM Portal.

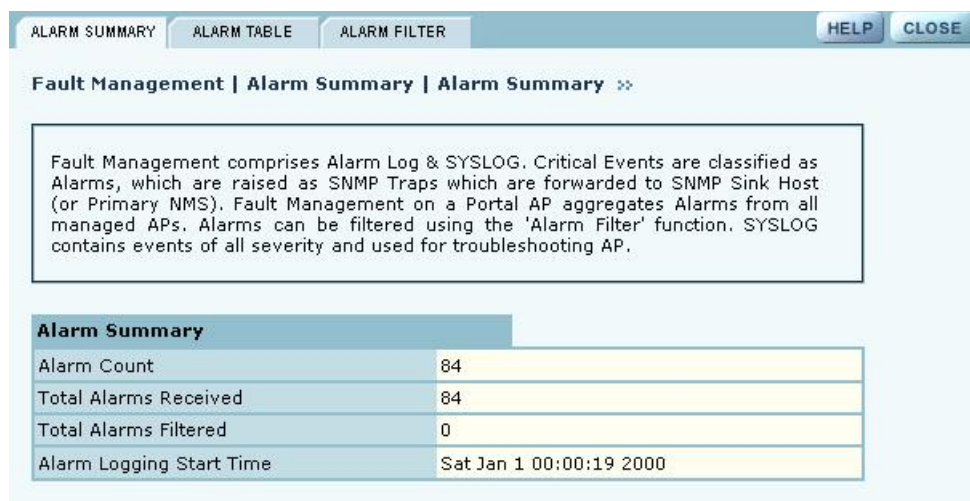


NOTE: The alarm count in the lower left corner of the Network Management Explorer window is the same as that given on the Alarm Summary tab. Click the Alarm Summary hyperlink to open the Alarm Summary tab.

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 146: Fault Management - Alarm Summary



Alarm Table

The Alarm Table tab (Figure 147) 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 196 and additional details are presented in Appendix C, “Alarms.”

The Alarm Table includes the following information:

Field	Description
Alarm ID	Text description of the specific alarm
Alarm From	Device ID of the AP that reported the alarm

Field	Description
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 that is 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 147: Fault Management - Alarm Summary - Alarm Table

ALARM SUMMARY
ALARM TABLE
ALARM FILTER
HELP
CLOSE

Fault Management | 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 (WSM)

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 14: 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 re-discovered 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 182). If this alarm occurs, NM Portal ceases to discover nor 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 other 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 a 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 14: Airgo Access Point Alarms (continued)

Alarm ID	Description
STA Association Failed	Generated when a 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 AP is not broadcasting SSID in beacon (due to suppressed SSID or multiple SSIDs being configured) and station is associating with AP with a different SSID. 7 - Authentication and encryption requested by station does not match security policy of the AP 8 - Multi Vendor Station are 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 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 used and the MAC address otherwise.
STA Disassociated	Generated when a 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 14: 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 authentication.
User Reject by RADIUS Server	Generated when user authentication fails. The AP radio and the RADIUS server which rejected the user are included in the message.
BP rejected by RADIUS Server	Generated when 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 14: 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 reset 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 Airgo 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 EAPOL key exchange process with a BP radio.

Table 14: 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 an 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 an 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 lockdown period started	Generated when a TKIP counter measures lockdown 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 14: 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 802.1x 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 a 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 148) 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 148: Fault Management - Alarm Summary - Alarm Filter

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](#)

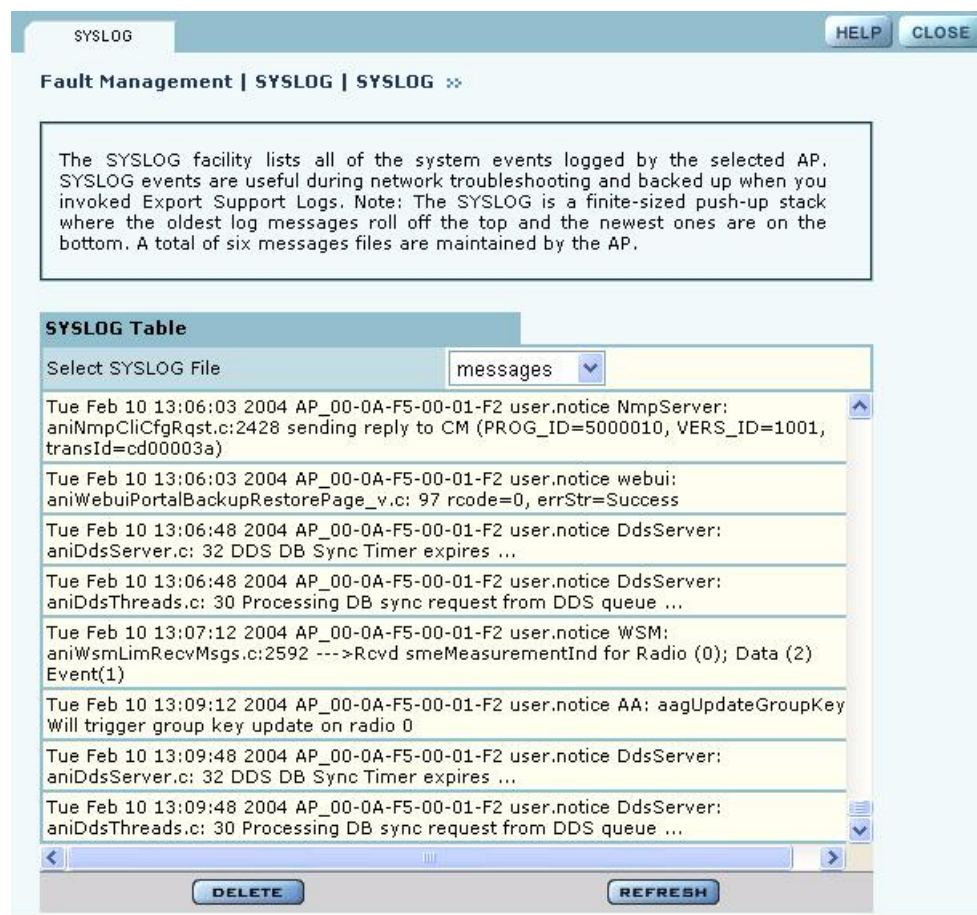
Add Events To Event-Filter-Table

Event ID: [v](#)

[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 149). See “Syslog Configuration” on page 211 for instructions on configuring the syslog message output.

Figure 149: Fault Management - SYSLOG

Managing Users

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 three 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 153.

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 150).

Figure 150: Security Portal - User Management - Wireless Users

Security Portal function of this AP manages User Accounts in RADIUS database. There are three types of users: wireless users, administrator users, and MAC-ACL users. Security Portal database should be backed up periodically. Also, it is recommended to nominate a redundant Security Portal in the network, whose database will be periodically mirrored with this database.

Login ID	User Name	User Group	Last Modified Date
☐ mlamb	Mary Lamb	employee	Tue Feb 10 13:24:48 2004

ADD DELETE MODIFY DETAILS

To add a new user, click **Add** to open the Add Wireless User entry panel (Figure 151).

Figure 151: Security Portal - User Management - Add Wireless User

Add a wireless user by specifying his/her login name, the user-group they belong to (which is later used in providing custom service levels to these users) and other optional attributes. The built-in certificate authority will generate a self-signed digital certificate which needs to be installed on client PC. Additionally, the WPA with EAP-TLS mode of security is required to be configured on all APs and Clients.

Add Wireless User

Login Name * mlamb

User Group employee

New User Group ☐

User First Name Mary

User Last Name Lamb

E-mail ID * mlamb@DeerCreekCo.com

Description

ADD RESET CANCEL

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, then 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 152).
 - 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 152: Security Portal - User Management - View Wireless User

View Wireless User	
Login Name	dyee
User Group	Employee
User First Name	Dawn
User Last Name	Yee
E-mail ID	dyee@xyzcompany.com
Description	
User Password	2_0Xi7Gq
Certificate	Click here to download certificate.

[< BACK](#)

Adding Administrative Users

To give designated users access to NM Portal, open the Admin Users tab (Figure 153).

Figure 153: Security Portal - User Management - Admin Users

WIRELESS USERS ADMIN USERS MAC ACLs GUEST USER ? 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
☐	mlamb	Mary Lamb	Administrator	Sun Jan 18 16:33:52 2004

[ADD](#)
[DELETE](#)
[MODIFY](#)
[DETAILS](#)

[COMMIT TO DATABASE](#)

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 154):

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 154: Security Portal - User Management - Add Administrative User

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 155) 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 155: 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	User Name	User Group	Last Modified Date
☐ 00:e0:98:7c:4c:6e	Hewlett Packard	employee	Sun Jan 18 14:09:04 2004
☐ 00:e0:98:7c:4c:6f	Packard Neighbor	employee	Sun Jan 18 14:10:04 2004

ADD DELETE MODIFY DETAILS COMMIT TO DATABASE

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 User entry panel (Figure 156):

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 156: Security Portal - User Management - Add MAC Address User

Add MAC Address Based User

MAC Address * 00 0A F5 00 60 10

User Group Employee New User Group ☐

User First Name Mary

User Last Name Lamb

E-mail ID mlamb@xyzcompany.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.

10 Maintaining the Access Point

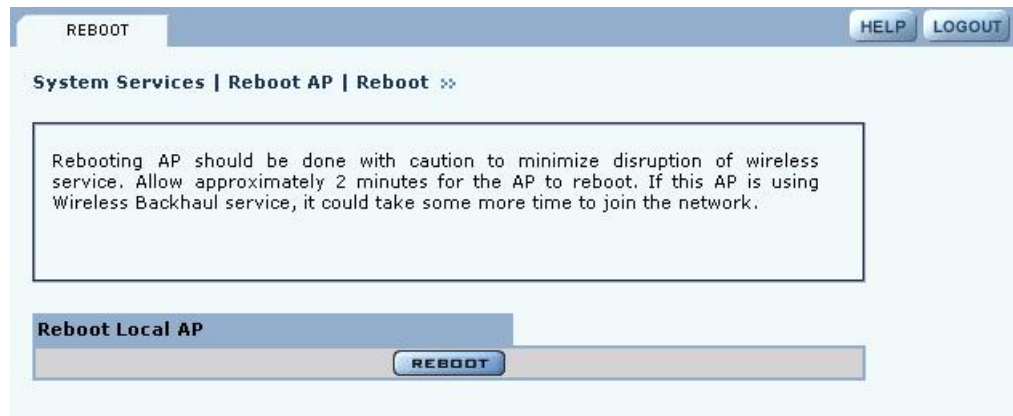
This chapter describes the tools available to maintain the Airgo Access Point. It contains the following sections:

- [Rebooting the AP](#)
- [Managing the System Configuration](#)
- [Click Apply to save the entries or Reset to return to the previously saved values.](#)
- [Upgrading Software](#)
- [Common Problems and Solutions](#)

Rebooting the AP

Choose **Reboot AP** from the System Services menu to order a reboot of the access point. To begin the process, click **Reboot** (Figure 158). The process takes approximately 2 minutes, and may take additional time if the AP is currently used for wireless backhaul service.

Figure 157: System Configuration - Reboot AP



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—Set up the real time clock (RTC) to keep track of time in the event that power is lost to 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 158) to update the IP and basic system configuration for the Airgo AP.

Figure 158: System Configuration - IP Configuration

The screenshot shows a web interface for configuring an Airgo Access Point. At the top, there are tabs: IP CONFIG, SYSLOG CONFIG, LICENSE MGMT, NMS CONFIG, and HW OPTIONS. The IP CONFIG tab is selected. To the right of the tabs are buttons for HELP and LOGOUT. Below the tabs, the breadcrumb path is 'System Services | System Configuration | IP Configuration >>'. A text box contains instructions: '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).' Below this, there are two main sections: 'Management IP Configuration' and 'System Identity Configuration'. The 'Management IP Configuration' section has four fields: 'DHCP Assigned IP Address' with a checked 'Enable' checkbox, 'DNS IP Address *' with the value '192.168.168.1', 'Management IP Address/Maskbits *' with the value '192.168.168.24/24', and 'Gateway IP Address *' with the value '192.168.168.254'. There are 'APPLY' and 'RESET' buttons below these fields. The 'System Identity Configuration' section has three fields: 'Host Name *' with the value 'AP_00-0A-F5-00-01-F2', 'AP Location' with the value 'Floor 1 South', and 'Administrator Contact' with the value 'admin@DeerCreekCo.com'. There are also 'APPLY' and 'RESET' buttons below these fields.

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 email address of the administrative contact for the AP.

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 159) provides controls to set the logging level and scope for a variety of functional areas or modules.

Figure 159: 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 *

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 160) 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 restore the previous license key.

Figure 160: System Configuration - License Management

The screenshot shows the 'License Management' tab selected in the 'System Configuration' section. The interface includes a navigation bar with tabs: IP CONFIG, SYSLOG CONFIG, LICENSE MGMT (selected), NMS CONFIG, and HW OPTIONS. There are also 'HELP' and 'LOGOUT' buttons. Below the navigation bar, the page title is 'System Services | System Configuration | License Management'. A message box states: '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 input field reads 'e.g. T6PR88GJRHKC or T6PR-88GJ-RHKC'. At the bottom of the section are 'APPLY' and 'RESET' buttons.

NMS Configuration

Use the NMS Configuration tab (Figure 161) 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.

Figure 161: System Configuration - NMS Configuration

IP CONFIGSYSLOG CONFIGLICENSE MGMTNMS CONFIGHW OPTIONSHELPLOGOUT

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	192.168.168.24

APPLYRESET

Enter the following values to set the NMS configuration:

Field	Description
Primary Manager IP	Enter the IP address of the NM Portal or NMS Pro server responsible for managing the AP. (required)
Auxiliary Manager IP	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 162) 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 162: System Configuration - Hardware Options

IP CONFIG SYSLOG CONFIG LICENSE MGMT NMS CONFIG HW OPTIONS HELP LOGOUT

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 specify subsystems to default configuration.

Secure Backup

Perform the following functions on the Secure Backup tab (Figure 166):

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 on the AP disk, so it is recommended to 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 on the AP disk, so it is recommended to remove it.

Figure 163: Configuration Management - Secure Backup

Configuration Reports

Select any of the following configuration reports on this tab (Figure 164):

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 164: Configuration Management - Configuration Reports

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 165).

Figure 165: 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 to Default	1 Select Reset AP Startup Configuration Only or AP Configuration and Databases 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 166) 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.

Figure 166: 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 167).
- 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 167: 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, installed, and the AP is 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 an Airgo-defined 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.

 **NOTE:** It is important to perform software upgrades during a scheduled maintenance window. Upgrading takes approximately 4-5 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.

 **CAUTION:** Do not leave the Software Upgrade panel while download is taking place. Clicking 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 168). 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 168: 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 cause any damage to 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 168).

Status information is automatically updated every 10 seconds. The status information shows clearly the stage of the distribution process and identifies any problems. Table 15 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 2 minutes in 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 flash memory.

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, then all services 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 15 lists common problems that can occur along with recommended solutions.

Table 15: 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 Access Point power LED is on. Check the Ethernet cable connections to both the computer and to the AP. Make sure that the network adapter in the computer is working properly. Check to see whether the IP address is on the same subnet as the Access Point.

Table 15: Common Problems and Solutions

Symptom	Problem	Solution
Poor or lower than expected signal strength, as measured by wireless network adapters attempting to connect to the Access Point.	Access Point may be poorly placed, or external antenna not connected properly.	The Access Point 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 that it is connected securely to the Access Point.

A Using the Command Line Interface

This appendix explains how to access and interact with the command line interface (CLI). For detailed information on specific commands, see the CLI Reference Manual.

Using the Command Line Interface

To connect to the AP for command line interface access using Secure Shell (SSH), do the following:

- 1 Launch your SSH client application.



NOTE: SSH Communications provides an SSH client, <http://www.ssh.com>.

- 2 Type `ssh admin@<AP IP address>`, using the AP IP address assigned to the Access Point (or 192.168.1.254 by default) and press Return.

When connected, a screen opens similar to the one shown in Figure 169.

Figure 169: Access Point Serial Console Login Screen

```
192.168.1.254 - PuTTY
login as: admin
admin@192.168.1.254's password:

push-pop : ctrl-p
Commands : ?
hot-keys : ctrl-/ or ctrl-alt-37

command> sh
command> show
show> sys
show> system
system(show)> system-gr
system(show)> system-group

mgmt-ipaddress : 192.168.1.254/24
gateway       : 0.0.0.0
clock        : Sat Jan  1 00:26:29 2000
hostname     : AP_00-0A-F5-00-02-9A
time-sync-type : manual
ntp-servers  : clock.via.net ntp-cup.external.hp.com timekeeper.isi.edu
              navobs2.usnogps.navy.mil
timezone     : pst8pdt
```

- 3 Enter your login ID and press Return. When prompted next, enter your password. The factory default for administrator access is user name: `admin`. If the AP has not been initialized, the user name field is grayed out. The factory default password is shipped with the AP on a paper insert. Use the password from the insert to log in.

- 4 To see the list of available commands, type a question mark (?). For a list of hot keys (short cuts for console functions, press Ctrl-H.

There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either `show` or `config`.

Toggle between show and config modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.

- 5 To log out and close your connection to the command line interface, type `logout` at any prompt.

Using the Console Port for CLI Access

To connect to the AP for command line interface (CLI) access using the built-in console port, do the following:

- 1 Connect your computer to the AP console port using a serial DCE cable (this is typically a 9-pin-to-9-pin cable with the transmit and receive lines crossed over a null modem cable). A USB-to-Serial adapter may be required if the computer lacks a 9-pin serial port.
- 2 Launch your terminal emulation application. On PCs running Microsoft Windows operating systems, the Microsoft-provided application HyperTerminal will work fine. (This is accessed usually through `Programs > Accessories > Communications > HyperTerminal`. The remainder of this procedure assumes the use of HyperTerminal. Modify the procedures accordingly if using another application.)
- 3 Create a terminal connection profile if one does not already exist. Enter a descriptive name and select any icon from the list provided. Click **OK** when done.
If there is a working HyperTerminal connection profile, select that shortcut instead to launch the connection, and skip to step 7.
- 4 The Connect To screen displays. The important element there is to use the `Connect using:` drop down box, and select the serial port to which the AP is connected. Click OK when done.
- 5 Use the following port settings:
 - Bits per second: 115200
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- 6 Click OK when done. When connected, a screen opens similar to the one shown in Figure 169.
- 7 If the console login screen in the HyperTerminal does not open, press **Return** once or twice. If you still see nothing or garbage characters appears, check the cable connection and the terminal connection parameters.
- 8 Enter your login ID and press Return. When prompted next, enter your password. (The AP defaults are login `admin` and password: `password`, and login `opr` and password `opr` for operator (read-only) access.)

- 9 To see the list of available commands, type a question mark (?). For a list of hot keys (short cuts for console functions, press Ctrl-H.

There are two important modes in console access, one is *show* mode and the other is *config* mode. In show mode, examine the AP's configuration settings and status. Use config mode to change values. To go into either mode from the main `command>` prompt, type either `show` or `config`.

Toggle between show and config modes by pressing Ctrl-P. Leave a mode and return to the top level command prompt by typing `exit`.

To log out and close your connection to the command line interface, type `logout` at any prompt.

B Regulatory and License Information

This appendix contains the regulatory and license information specific to the Airgo Access Point hardware and software.

Table 16: Regulatory and License Compliance

ID	Access Point Requirement	Details
CERT1	Safety	UL 1950 third edition TUV approval UL-2043 (Fire and Smoke) Compliance
CERT2	EMC	EMC Directive 89/336/EEC (CE Mark)
CERT3	Radio Approvals	FCC CFR47 Part 15, section 15.247 FCC (47CFR) Part 15B, Class B Emissions Canada IC RSS210 Japan MPT Radio Regulations Europe: ETS 300.328

C Alarms

Alarms generated by the Airgo Access Point are stored persistently on the AP. The Airgo AP can store approximately $130 * 2 = 260$ alarms in total. When the number of alarms exceeds this limit, the oldest alarm set is discarded.

All alarms generated by the Airgo Access Point have the following parameters:

- **Event ID:** The internal event number that uniquely identifies the event.
- **Log-level:** The criticality of the event. All alarms are logged at the same criticality.
- **Log-time:** The time as determined by the clock on the Access point, when the alarm was logged. All forwarded alarms have the log-time set to the clock time on the originating Access point.
- **Module:** The subsystem on the Access point that generated the alarm.
- **Source:** The hostname or IP address of the access point that generated the alarm.
- **Description:** The alarm details.

Use the Airgo AP CLI to display the alarm table as follows:

Examples: `system(show) > alarm-table`

```
event-id   : 102
log-level  : 2
log-time   : Tue Jan  4 16:14:01 2000
module     : WSM
source-ip  : AP_00-0A-F5-00-02-1F
description : Device ID AP_00-0A-F5-00-02-1F radio 6 is enabled, its operational
              state is 2 operating on 11
-----
event-id   : 103
log-level  : 2
log-time   : Tue Jan  4 17:04:28 2000
module     : WSM
source-ip  : AP_00-0A-F5-00-02-1F
description : Device Id AP_00-0A-F5-00-02-1F radio 4 disabled
-----
```

The following section describes in detail the alarm syntax and alarm parameters. The alarm and its parameters together are shown as “description” above. The following alarms are described:

- “Discovery: Discovered new node” on page 235
- “Discovery: Node deleted from network” on page 235
- “Discovery: Managed nodes limit exceeded” on page 236
- “Enrollment: Node Enrolled” on page 236
- “Enrollment: Node Un-enrolled” on page 237
- “Policy: Policy Download Successful” on page 238

- “Policy: Policy Download Failed” on page 238
- “Software Download: Image Download Succeeded” on page 239
- “Software Download: Image Download Failed” on page 239
- “Software Download: Software Distribution Succeeded” on page 240
- “Wireless: Radio enabled (BSS Enabled)” on page 241
- “Wireless: Radio Disabled (BSS disabled)” on page 241
- “Wireless: BSS Enabling Failed” on page 242
- “Wireless: Frequency Changed” on page 242
- “Wireless: STA Association Failed” on page 243
- “Wireless: STA Associated” on page 244
- “Wireless: STA Disassociated” on page 245
- “Wireless: WDS Failed” on page 246
- “Wireless: WDS Up” on page 246
- “Wireless: WDS Down” on page 247
- “Security: Guest Authentication Succeeded” on page 248
- “Security: Guest Authentication Failed” on page 249
- “Security: User rejected by RADIUS Server” on page 249
- “Security: BP rejected by RADIUS Server” on page 250
- “Security: RADIUS Server timeout” on page 251
- “Security: Management User login success” on page 252
- “Security: Management User login failure” on page 253
- “Security: STA failed EAPOL MIC check” on page 253
- “Security: STA attempting WPA PSK – no Pre-shared Key is set for SSID” on page 254
- “Security: Auth Server Improperly configured on this SSID” on page 255
- “Security: STA failed to send EAPOL-Start” on page 256
- “Security: RADIUS sent a bad response” on page 256
- “Security: RADIUS timeout too short” on page 257
- “Security: STA authentication did not complete in time” on page 258
- “Security: Upstream AP is using an untrusted auth server” on page 259
- “Security: Upstream AP failed MIC check during BP authentication” on page 260
- “Security: Premature EAP-Success received” on page 261
- “Security: Profile not configured for user-group” on page 262
- “Security: STA has failed security enforcement check” on page 263
- “Security: Guest Authentication Failed” on page 264
- “Security: BP Detected Bad TKIP MIC on Incoming Unicast” on page 266
- “Security: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast” on page 266
- “Security: STA Detected Bad TKIP MIC on Incoming Unicast” on page 267
- “Security: STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast” on page 268
- “Security: TKIP counter-measures lockout period started” on page 268
- “Security: EAP response timeout” on page 270
- “Security: EAPOL Key exchange – message 2 timeout” on page 271
- “Security: EAPOL Group 2 key exchange timeout” on page 272

Discovery: Discovered new node

Alarm generated when a new Airgo AP is discovered in the network.

Syntax: `DeviceId %s discovered node [deviceId=%s, IP=%s, Subnet=%s].`

Alarm Parameters

DeviceID	The Portal's Device ID.
deviceId	The discovered node's device ID
IP	The discovered node's IP address
Subnet	The Subnet to which the discovered node belongs

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is generated when an Airgo AP is discovered by the NM Portal the first time.

Usage: Informational log.

Examples: `DeviceId AP_00-0A-F5-00-02-1F discovered node [deviceId=AP_00-0A-F5-00-01-B0, IP=192.168.75.244, Subnet=255.255.254.0].`

See Also: <Node deleted from network>

Discovery: Node deleted from network

Generated when a node is deleted from the Portal network.

Syntax: `DeviceId %s Node [Ip=%s, persona=%d] deleted from database.`

Alarm Parameters

DeviceId	The Device ID of the NM Portal
Ip	The IP address of the node being deleted.
Persona	The Persona of the node being deleted.

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is generated when the a discovered node is deleted from the system. When a node is deleted, all information about that node is erased from the Portal. If the node's IP address falls within the discovery scope, then the node will be re-discovered and added back to the set of the discovered nodes on the next discovery

sweep.

Usage: Informational log.

Examples: `DeviceId AP_00-0A-F5-00-02-1F Node [Ip=192.168.74.210, persona=6] deleted from database.`

See Also: <Discovered new node>

Discovery: Managed nodes limit exceeded

Generated when a the number of nodes discovered exceeds the predefined limit on the NM portal.

Syntax: `On Device %s Node[Ip=%s] managed node limit exceeded. Current managed nodes limit is %d.`

Alarm Parameters

Device	The Device ID of the NM Portal
IP	The IP address of the node being deleted.
Node Limit	The current limit imposed on the discovery server.

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is generated when the number of discovered nodes exceeds the predefined limit. The current limit on number of access points discovered is 50. This limit can be configured to be lower.

Usage: If this alarm occurs then the discovery server will not discover nor track any new nodes once this limit is reached. In such case, delete unwanted nodes and manually add the nodes to the discovery database so that they may be managed.

Examples: `On Device AP_00-0A-F5-00-02-1F Node[Ip=192.168.74.245] managed node limit exceeded. Current managed nodes limit is 10.`

See Also:

Enrollment: Node Enrolled

Alarm generated when an Airgo AP is enrolled into the network

Syntax: `NMPortal with DeviceId %s has successfully enrolled a remote node having ApDeviceId=%s NodeIp=%s and Persona=%d`

Alarm Parameters

DeviceId	The Device ID of the NMPortal
ApDeviceId	The Device ID of the remote AP

NodeIp The IP address of the remote AP

Persona The Persona of the remote AP
 6 = Security Portal
 2 = Normal AP

Alarm Severity

Severity Critical

Description: This alarm is generated when the Airgo AP has been successfully enrolled into the network.

Usage: Informational log.

Examples: NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2

See Also: <Node Unenrolled>

Enrollment: Node Un-enrolled

Alarm generated when the Airgo AP is rejected (un-enrolled) from the network

Syntax: NMPortal with **DeviceId** %s has successfully unenrolled the remote node having **ApDeviceId**=%s **NodeIp**=%s and **Persona**=%d

Alarm Parameters

DeviceId The Device ID of the NMPortal

ApDeviceId The Device ID of the remote AP

NodeIp The IP address of the remote AP

Persona The Persona of the remote AP
 6 = Security Portal
 2 = Normal AP

Alarm Severity

Severity Critical

Description: This alarm is generated when the Airgo AP has been successfully rejected (un-enrolled) from the network.

Usage: Informational log.

Examples: NMPortal with DeviceId AP_00-0A-F5-00-01-77 has successfully enrolled a remote node having DeviceIdId=AP_00-0A-F5-00-01-7A NodeIp=172.16.12.4 and persona=2

See Also: <Node Enrolled>

Policy: Policy Download Successful

Alarm generated when a policy is successfully downloaded to an AP.

Syntax: For accesspoint **Node** %s The **policy** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name
from	The device ID of the source of the policy
time	The time at which the policy was consumed

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is generated when a policy is successfully downloaded to an AP.

Usage: Informational log.

Examples: For accesspoint Node AP_00-0A-F5-00-01-77 The policy [security.xml] from [TrustedManager] was successfully downloaded at time[Thu Jan 6 04:27:45 2000]

See Also: <Policy Download Failed>

Policy: Policy Download Failed

Alarm generated when a policy is download to an AP failed.

Syntax: For accesspoint **Node** %s the **policy** [%s] **from** [%s] could not be downloaded due to **error** %d at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
policy	The policy name
from	The device ID of the source of the policy
error	The failure error code
time	The time at which the policy was consumed

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is sent when a policy downloaded to an AP could not be consumed correctly either due to an error in the policy or software version mismatch or due to some other error.

Usage: Informational log.

Examples: For accesspoint Node AP_00-0A-F5-00-01-7D The policy [defaultpolicy.xml] from [TrustedManager] could not be downloaded due to error 22549 at time[Wed Feb 11 17:28:38 2004]

See Also: <Policy Download Successful>

Software Download: Image Download Succeeded

Alarm generated when an image is successfully downloaded and applied to an AP.

Syntax: For accesspoint **Node** %s the software **image** [%s] **from** [%s] was successfully downloaded at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version information
from	The device ID of the source of the image
time	The time at which the image was consumed

Alarm Severity

Severity	Critical
----------	----------

Description: This alarm is when an image is successfully downloaded and applied to an AP.

Usage: Informational log.

Examples: For accesspoint Node AP_00-0A-F5-00-01-77 The software image [1.1.0, build 3278, AGN1dev, Airgo Inc.,] from [AP_00-0A-F5-00-01-77] was successfully downloaded at time[Fri Jan 7 06:04:47 2000]

See Also: <Image Download Failed, Software Distribution Succeeded>

Software Download: Image Download Failed

Alarm generated when an image is un-successfully downloaded and applied to an AP.

Syntax: For accesspoint **Node** %s The software **image** [%s] **from** [%s] could not be downloaded due to **error** %d at **time**[%s]

Alarm Parameters

Node	The device ID of the remote AP
image	The image version

from The device ID of the source of the image

error The failure error code

time The time at which the error occurred

Alarm Severity

Severity Critical

Description: This alarm is when an image is un-successfully downloaded and applied to an AP.

Usage: Image download failures can happen due to corrupted images, invalid length images or due to connectivity failures.

Examples: For accesspoint Node AP_00-0A-F5-00-01-77 The software image [] from [AP_00-0A-F5-00-01-77] could not be downloaded due to error 24581 at time[Fri Jan 7 04:12:35 2000]

See Also: <Image Download Succeeded, Software Distribution Succeeded>

Software Download: Software Distribution Succeeded

Alarm generated when an image distribution is completed.

Syntax: On **DeviceId** %s, the Software **image** [%s] distribution request from **portal**[%s] using the Distribution **TaskId**=%s and with **status**=%s completed at **time**[%s]

Alarm Parameters

DeviceId The device ID of the remote AP

image The image version

portal The device ID of the source of the image (NMS or NMPortal)

TaskId The task ID of the distribution

status The distribution status (success or failure) of the selected APs

time The time at which the distribution was done

Alarm Severity

Severity Critical

Description: This alarm is when an image distribution is completed. Image distribution is

Usage: Informational log.

Examples: On DeviceId AP_00-0A-F5-00-01-77 , the Software image [0.7.0, build A.2286, AGN1dev, Airgo Inc.,] distribution request from portal[AP_00-0A-F5-00-01-77] using the Distribution TaskId=000000 and with status=172.16.12.4, , 0, 947304168, 947304183, invalid image file. completed at time[Tue Jan 6 21:32:18 1970]

See Also: <Image Download Failed, Image Download Succeeded>

Wireless: Radio enabled (BSS Enabled)

Notification which indicates that AP radio has been enabled.

Syntax: "Device ID %s radio %d is enabled, its operational state is %d operating on %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
Operational Mode	This indicates the operational mode of the radio whether it is 802.11a, 802.11b or 802.11g
Channel ID	This indicates the channel on which the AP is operating.

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which is generated when a AP radio (BSS) is enabled

Usage: This indicates successful start of a BSS and also provides the channel on which the AP radio will be operating on.

Examples: Device ID AP_00-0A-F5-00-01-B6 radio 4 is enabled, its operational mode is 1 and operating on 64

See Also:

Wireless: Radio Disabled (BSS disabled)

Notification which indicates that the AP radio has been disabled.

Syntax: "Device Id %s radio %d disabled"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which indicates that AP has been disabled.

Usage: The AP radio can be disabled for several reasons such as:
a. User Triggered (administrative disabling)

- b. Radio reset caused due to application of wireless specific configuration
- c. Radio reset triggered by hardware
- d. Radio reset due to change in SSID

Examples: Device Id AP_00-0A-F5-00-01-B6 radio 4 disabled

See Also: <List of other alarms>

Wireless: BSS Enabling Failed

Notification which indicates that the AP radio (BSS) enabling failed.

Syntax: “Bss enabling failed for DeviceId %s radio %d CauseCode %d”

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
Cause Code	Reason for AP radio enabling failure

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which indicates that AP rado enabling has failed

Usage: The AP radio enabling can fail for reasons which are indicated by the Cause code parameter:

0 – Unspecified reason

1 – System timeout attempting to enable BSS.

Examples: Bss enabling failed for Device Id AP_00-0A-F5-00-01-B6 radio 4 Cause Code 1

See Also: <List of other alarms>

Wireless: Frequency Changed

Notification which indicates that the frequency of operation changed on the AP.

Syntax: "Frequency changed for DeviceId %s radio %d channelId %d CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
----------	-------------------------------

Radio	Identifies Radio by interface ID on the Access Point
Channel ID	This indicates the channel on which the AP is operating.
Cause Code	Reason why frequency changed

Alarm Severity

Severity	Critical
----------	----------

Description: This is a notification generated when operating frequency is changed for an AP radio due to either user triggers or events such as periodic DFS. The reason code can have an value of 0 which is unspecified reason. The new channel ID is also provided.

Reason Code	Description
0	Triggered due to DFS
1	User Triggered

Usage: This is an informational log.

Examples: Frequency Changed for Device ID AP_00-0A-F5-00-01-B6 radio 4 channelId 64 CauseCode 0

See Also:

Wireless: STA Association Failed

Notification which indicates that the association failed for a 802.11 station.

Syntax: "Station association failed for DeviceId %s radio %d station MAC %s station status %d CauseCode"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
STA status	Association or reassociation
Cause Code	Reason why station association failed

Alarm Severity

Severity	Critical
----------	----------

Description: This is a notification generated when a association from a 802.11 station fails with the AP radio. The reasons for the failure are encapsulated in the cause code parameter and are as follows:

- 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 AP is not broadcasting SSID in beacon (either due to SSID being suppressed or multiple SSIDs being configured) and station is associating with AP with a different SSID.
- 7 - Authentication and encryption requested by station does not match security policy of the AP
- 8 - Multi Vendor Station are 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 transferred to another AP Radio due to Load Balancing
- 11 - Station is not allowed to associate because node does not have network connectivity

Usage: The reason for the association failure can be used to determine any configuration issue in the system which may be causing the association failures.

Examples: Station association failed for Device ID AP_00-0A-F5-00-01-B6 radio 4 station MAC 00:0a:f5:00:3a:fe CauseCode 2

See Also:

Wireless: STA Associated

Notification which indicates that the association and authentication was successful for a 802.11 station.

Syntax: "Station associated for DeviceId %s radio %d station MAC %s, Station status %d userId %s station count %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
STA status	Association or reassociation
User ID	Identifies user by user name or MAC address
Station Count	Current count of associated users with AP.

Alarm Severity

Severity Critical

Description: This is a notification generated when a association and authentication from a 802.11 station succeeds with the AP radio. In addition count of current associated stations, type of association and user ID is provided. User ID is user name if RADIUS authentication is used and MAC address otherwise.

Usage: Informational log.

Examples: Station associated for Device ID AP_00-0A-F5-00-01-B6 radio 4 station MAC 00:0a:f5:00:3a:fe, Station status 1 userId John Doe station count 10

See Also:

Wireless: STA Disassociated

Notification which indicates that a 802.11 station disassociated.

Syntax: "Station disassociated from AP for DeviceId %s radio %d station MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
STA MAC Address	MAC address of 802.11 station.
Cause Code	Reason Code for disassociation

Alarm Severity

Severity Critical

Description: This is a notification generated when a 802.11 station is disassociated either by the network or the station.

Reason Code	Description
0	STA 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.

Usage: Informational log.

Examples: Station disassociated for Device ID AP_00-0A-F5-00-01-B6 radio 4 station MAC 00:0a:f5:00:3a:fe, CauseCode 0

See Also:

Wireless: WDS Failed

Notification which indicates a failure in formation of Wireless Backhaul

Syntax: "WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Reason Code for WDS formation failure

Alarm Severity

Severity	Critical
----------	----------

Description: This is a notification generated when a wireless backhaul formation fails. The remote end's MAC address is provided. This notification is generated by AP node.

Reason Code	Description
0	System Failure
1	Maximum BP count has been reached (this relevant only for AP)
2	Join attempt to the uplink AP failed (relevant only on BP side)

Usage: This can be used to track any losses in connectivity of network.

Examples: WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4 remote MAC 00:0a:f5:00:3a:fb, CauseCode 0

See Also:

Wireless: WDS Up

Notification which indicates successful formation of wireless backhaul

Syntax: "WDS trunk established for DeviceId %s radio %d remote mac %s TrunkPort count %d CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
----------	-------------------------------

Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Backhaul Count	Number of backhauls which are formed to this AP radio
Cause Code	Indicates whether backhaul was a retrunk or not

Alarm Severity

Severity	Critical
----------	----------

Description: This is a notification generated when a wireless backhaul formation succeeds. The remote end's MAC address is provided.

Reason Code	Description
0	Trunk has been established
1	Trunk has been optimized (re-established based on better connectivity)

Usage: Informational log

Examples: WDS trunk established for Device ID AP_00-0A-F5-00-01-B6 radio 4
remote MAC 00:0a:f5:00:3a:fb TrunkPort count 2 CauseCode 0

See Also:

Wireless: WDS Down

Notification which indicates that a wireless backhaul link has gone down

Syntax: "WDS trunk brought down for DeviceId %s radio %d remote MAC %s CauseCode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
Remote MAC Address	MAC address of remote end of backhaul link
Cause Code	Indicates why backhaul link was brought down

Alarm Severity

Severity	Critical
----------	----------

Description: This is a notification generated when a wireless backhaul has gone down. The remote end's MAC address is provided.

Reason Code	Description
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 retronk 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) |

Usage: Informational log

Examples: WDS trunk brought down for Device ID AP_00-0A-F5-00-01-B6 radio 4 remote MAC 00:0a:f5:00:3a:fb CauseCode 0

See Also:

Security: Guest Authentication Succeeded

Notification which indicates that a “Guest Access” Station has been successfully authenticated

Syntax: "For device-id %s , Guest authentication succeeded for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.

Alarm Severity

Severity	Normal
----------	--------

Description: Notification which is generated when a “Guest Station” is authenticated.

Usage: This indicates the successful start of a “Guest Access” Stations communications session. This Guest STA will be offered the communications services specified in the Guest Profilethat has been configured for the specified SSID.

Examples: For device-id AP_00-0A-F5-00-01-89 , Guest authentication succeeded for STA 00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and guest mode 4

See Also: `Security: Guest Authentication Failed`

Security: Guest Authentication Failed

Notification which indicates that a “Guest Access” Station has failed authentication

Syntax: "For device id %s, Guest authentication failed for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d due to %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.
Reason code	Currently, always set to 0.

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which is generated when a “Guest Station” fails authentication.

Usage: This indicates that a Guest Station did not present the appropriate “credentials” (currently simple password) upon request.

Examples: For device-id AP_00-0A-F5-00-01-89 , Guest authentication failed for STA 00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and guest mode 4 due to 0

See Also: `Security: Guest Authentication Succeeded`

Security: User rejected by RADIUS Server

Notification which indicates that the AP has determined that a User has been rejected by RADIUS.

Syntax: "For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the STA %s on radio %d with user-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the Auth Zone on this AP that this RADIUS server is a member of
Station	MAC address of the Station
Radio	Identifies Radio by interface ID on the Access Point
User ID	The Username
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when a User authentication fails. The context of the AP radio and the RADIUS server which rejected the User are also provided.

Usage: This indicates that the AP has determined that RADIUS has rejected a user authentication attempt.

Examples: For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from auth zone BldgOne rejected rejected the STA 00:0a:f5:00:05:cc on radio 0 with user-id paul and SSID NewYorkRm

See Also:

Security: BP rejected by RADIUS Server

Notification which indicates that the AP has determined that a RADIUS server has rejected this BP's authentication attempt.

Syntax: "For device-id %s, the RADIUS SERVER %s:%d from auth zone %s rejected the node %s on radio %d with device-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the auth Zone on this AP that this RADIUS server is a member of

Node	MAC address of the BP node
Radio	Identifies Radio by interface ID on the Access Point
Device ID	The Device ID of the BP node
SSID	Identifies the SSID on this AP that the STA has associated with
Alarm Severity	
Severity	Critical

Description: This notification is generated when a Bridge Portal (radio) authentication fails. The context of the BP radio and the RADIUS server which rejected the BP radio are also provided. A BP attempts authentication when a wireless backhaul is being established.

Usage: This indicates that a security portal has rejected a BP's authentication attempt with this AP. Usually it means that the BP is not enrolled in the same network as the AP. It may also mean that the BP was just enrolled, and the enrollment database has not yet been synced across the network to all security portals.

Examples: For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from auth zone BldgOne rejected the node 00:0a:f5:00:06:22 on radio 0 with device-id AP_00-0A-F5-00-01-89 and SSID NewYorkRm

See Also:

Security: RADIUS Server timeout

Notification which indicates that the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout.

Syntax: "For device-id %s, the RADIUS server %s:%d from auth zone %s failed to respond within %d seconds and %d attempts while authenticating STA %s on radio %d with user-id %s and SSID %s"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Auth Zone	The name of the auth Zone on this AP that this RADIUS server is a member of
RADIUS timeout	The current setting of the RADIUS timeout.
RADIUS retries	The number of retries performed
Station	MAC address of the Station.

Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when the RADIUS server fails to respond within a certain timeout period.

Usage: This indicates that the AP has determined that a RADIUS server has failed to respond within the RADIUS timeout. This may mean that the RADIUS server is unreachable over the network, or the shared secret with the RADIUS server is misconfigured on the AP. Usually, RADIUS servers do not respond when clients attempt to communicate with bad shared secrets. If multiple RADIUS servers are configured in this auth zone, the AP will switch to using the next one in the list.

Examples: For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 from auth zone BldgOne failed to respond within 5 seconds and 3 attempts while authenticating STA 00:0a:f5:00:05:f0 on radio 0 with user-id paul and SSID NewYorkRm

See Also:

Security: Management User login success

Notification which indicates that the AP has determined that a Management user login has succeeded.

Syntax: "For device-id %s, the management user '%s' with privilege level %d logged in successfully via %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Management User	Username of management User.
Privilege Level	The privilege level of the management user (Ignore in this release.)
Login access	Identifies the type of access, console, or SSH. (Ignore in this release.)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated whenever a management User tries to login to the local AP.

Usage: This indicates that the AP has determined that a Management user login has

succeeded.

Examples: For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' with privilege level 1 logged in successfully via 1

See Also:

Security: Management User login failure

Notification which indicates that the AP has determined that a Management user login has failed.

Syntax: "For device-id %s, the management user '%s' failed to login successfully via %d"

DeviceId	The Device ID of the Airgo AP
Management User	Username of management User.
Login access	Identifies the type of access, console, or SSH. (Ignore in this release.)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when a management User login attempt is unsuccessful.

Usage: This indicates that the AP has determined that a Management user login has failed. Too many failed logins in succession might attempt that someone is trying to break into your AP.

Examples: For device-id AP_00-0A-F5-00-01-89 , the management user 'admin' failed to login successfully via 1

See Also:

Security: STA failed EAPOL MIC check

Notification which indicates that the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user-id %s and SSID %s failed an EAPOL-MIC check with auth-type %d during key exchange %d. (If using WPA-PSK, check the PSK on the STA.)"

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point

User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: WPA PSK (3), WPA EAP (4)
Key Exchange	0 for pairwise key exchange, and 1 for group key exchange.
Alarm Severity	
Severity	Critical

Description: This notification is generated when the MIC fails during EAPOL key exchange process.

Usage: This indicates that the AP has determined that a STA has failed a MIC check during the EAPOL authentication exchange. If the authentication type is WPA PSK, and the failure happened during the pairwise key exchange, then this is most likely due to a misconfiguration of the WPA pre-shared key on the station. Otherwise, it might mean that an attacker's station is attempting to masquerade as a legal station.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm failed an EAPOL-MIC check with auth-type 4 during key exchange 2. (If using WPA-PSK, check the PSK on the STA.)

See Also:

Security: STA attempting WPA PSK – no Pre-shared Key is set for SSID

Notification which indicates that the AP has determined that a STA is attempting WPA-PSK authentication – but no Pre-shared Key has been configured for the SSID.

Syntax: "For device-id %s, the STA %s on radio %d attempted to do WPA-PSK based auth on the SSID %s but no pre-shared key is set."

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is sent when a Station attempts to do a WPA-PSK based

Usage: authentication on a given SSID, but no WPA pre-shared key is setup for that SSID. This indicates that the AP has determined that a STA is attempting to perform WPA-PSK authentication – but no WPA Pre-shared Key has been configured on this AP for that SSID. Recall that WPA PSK's are configured per SSID.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 attempted to do WPA-PSK based auth on the SSID NewYorkRm but no pre-shared key is set.

See Also:

Security: Auth Server Improperly configured on this SSID

Notification which indicates that the AP has determined that a STA requires authentication servers – and these are not configured properly on this SSID.

Syntax: "For device-id %s, Auth servers are improperly configured for the SSID %s and are needed for authenticating STA %s on radio %d with RADIUS usage %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
SSID	Identifies the SSID on this AP that the STA has associated with
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
RADIUS Usage	A code indicating what the RADIUS server was required for: Legacy 8021.x for dynamic WEP (1), WPA EAP authentication (2), MAC address based ACL lookup (3).

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is sent when authentication servers are improperly configured for a given SSID.

Usage: This indicates that the AP has determined that a STA requires authentication servers configured –and there are none configured on this SSID Generally authentication servers are needed for EAP based authentication, or for MAC address based ACL lookups.

Examples: For device-id AP_00-0A-F5-00-01-89 , Auth servers are improperly configured for the SSID NewYorkRm and are needed for authenticating STA 00:0a:f5:00:05:f0 on radio 0 with RADIUS 2

See Also:

Security: STA failed to send EAPOL-Start

Notification which indicates that the STA has failed to send an EAPOL-Start even though it was expected to for EAP based authentication.

Syntax: "For device-id %s, the STA %s on radio %d and SSID %s failed to send an EAPOL-Start in order to begin auth of type %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: LEGACY 802.1x (2), WPA EAP (4)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is sent during authentication, when the Station fails to send an EAPOL-Start in order to begin the authentication using WPA-EAP or legacy 802.1X protocols.

Usage: This indicates that the AP has determined that a STA has failed to send an EAPOL-Start. This might indicate a misconfiguration on the STA. The AP expects the STA 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.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 on radio 0 and SSID NewYorkRm failed to send an EAPOL-Start in order to begin auth of type 4

See Also:

Security: RADIUS sent a bad response

Notification which indicates that the AP has determined that a RADIUS server has sent a bad response.

Syntax: "For device-id %s, the RADIUS server %s:%d sent back a bad response due to %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
----------	-------------------------------

RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
Response	The reason codes for the bad response: BAD SIGNATURE BASED ON SHARED SECRET (0), UNEXPECTED RESPONSE TYPE WHEN DOING EAP AUTH (1), UNEXPECTED RESPONSE TYPE WHEN DOING MAC-ACL LOOKUP (2), LEGAL MS-MPPE KEYS NOT PRESENT (3), BAD ENCODING FOR USER GROUP ATTRIBUTE (5)

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is sent during authentication, when the RADIUS server sends a bad response. The aniNotifCauseCode identifies the reason associated with this bad response.
- Usage:** This indicates that the AP has determined that a RADIUS server has sent a bad or unexpected response. The response could be bad because the cryptographic signature check might have failed or because an attribute might be missing or badly encoded.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 sent back a bad response due to 7

See Also:**Security: RADIUS timeout too short**

Notification which indicates that the AP has determined that a RADIUS server has sent a late response. This indicates that the APs RADIUS timeout might need to be increased.

- Syntax:** "For device-id %s, the RADIUS server %s:%d sent a late response - you might need to increase your RADIUS timeout of %d seconds"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
RADIUS server	The IP address of the RADIUS server.
Port	The port used to communicate with the RADIUS server.
RADIUS timeout	The current setting of the RADIUS timeout.

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when the AP receives a late response from the

RADIUS server, as opposed to not receiving any response at all. The AP may have attempted multiple retries or may even have switched to another RADIUS server by this time. This indicates that due to higher latencies in the network, it might be better to increase the timeout associated with the authentication server.

Usage: This indicates that the AP has determined that a RADIUS server has sent a late response.

Examples: For device-id AP_00-0A-F5-00-01-89 , the RADIUS server 192.168.75.230:1812 sent a late response - you might need to increase your RADIUS timeout of 4 seconds

See Also:

Security: STA authentication did not complete in time

Notification which indicates that the AP has determined that a station has failed to complete the proper sequence of authentication exchanges in a timely manner.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not complete its auth sequence in time with auth-type %d and enc-type %d due to reason code %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
AP	The MAC address of the upstream AP.
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID, if exchanged the during EAPOL authentication
SSID	Identifies the SSID on this AP that the STA has associated with
Authentication Type	The valid types include: LEGACY 802.1x (2), WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)
Reason Code	The reason for the failure: EAP-REQUEST NOT RECEIVED FROM AUTHENTICATION SERVER (2)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when the station authentication sequence did not complete in time.

- Usage:** This indicates that the AP has determined that the station authentication sequence did not complete in time.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not complete its auth sequence in time with auth-type 4 and enc-type 6 due to reason code 6
- See Also:** EAP User-ID timeout, EAP Response Timeout

Security: Upstream AP is using an untrusted auth server

Notification which indicates that the local BP has determined that the upstream AP is using an untrusted auth server.

- Syntax:** "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d is using an untrusted auth server %s with certificate SHA-1 thumbprint %s : IT MIGHT BE A ROGUE AP"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Node	The Device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 Thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when the local BP has determined that the upstream AP is using an un-trusted auth server.
- Usage:** This indicates that the local BP has determined that the upstream AP is using an un-trusted auth server. This may indicate that the upstream AP is a rogue AP. It is safe to say that the upstream AP and the downstream AP are not enrolled in the same network. If the downstream AP was previously enrolled elsewhere, then reset it and re-enroll it in the new network.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 is using an untrusted auth server 00:0a:f5:00:01:45 with certificate SHA-1 thumbprint 98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e : IT MIGHT BE A ROGUE AP
- See Also:**

Security: Upstream AP is using a non-portal node as its auth server

Notification which indicates that the local BP has determined that the upstream AP is using a non-portal node as an auth server.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d is using a non portal node %s with certificate SHA-1 thumbprint %s as its auth server: YOUR ENROLLMENT DATABASE MIGHT BE OUT OF SYNC."

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Node	The Device ID (X.509 Certificate CN) of the entity used by the upstream AP as an auth server
Thumbprint	The SHA-1 Thumbprint of the certificate for this purported portal

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when the local BP has determined that the upstream AP is using a node that is not a security portal as its auth server. This indicates that the BP knows about the other Airgo node, but does not believe it is authorized to be a Security Portal.

Usage: This indicates that the local BP has determined that the upstream AP is out-of-sync with respect to the identity of legitimate portal APs and the enrollment databases are out of sync on the downstream AP and the upstream AP.

Examples: For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 is using a non portal node 00:0a:f5:00:01:45 with certificate SHA-1 thumbprint 98:72:a8:6d:56:f8:92:a8:f3:97:ec:3f:fa:0b:66:4e as its auth server: YOUR ENROLLMENT DATABASE MIGHT BE OUT OF SYNC

See Also:

Security: Upstream AP failed MIC check during BP authentication

Notification which indicates that the local BP has determined that the upstream AP has failed a MIC check on a received frame.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via

local BP radio %d failed an EAPOL-MIC check with auth-type %d during key exchange %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point
Authentication Type	The valid types include: RSN PSK (3), RSN EAP (4)
Key Exchange	Pairwise key exchange (0), group ky exchange (1).

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when the MIC fails during EAPOL key exchange process via a BP radio.

Usage: This indicates that a frame with a MIC failure has been received during the EAPOL Key Exchange process.

Examples: For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 failed an EAPOL-MIC check with auth-type 4 during key exchange 3

Security: Premature EAP-Success received

Notification which indicates that the local BP has received an EAP-Success BEFORE authentication has completed.

Syntax: "For device-id %s, the upstream AP %s with SSID %s authenticating via local BP radio %d sent EAP-Success before authentication completed : IT MIGHT BE A ROGUE AP"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
AP	The MAC address of the upstream AP.
SSID	Identifies the SSID on this AP that the STA has associated with.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when an upstream AP sends an EAP success before authentication is completed. This may be a rogue AP trying to force an AP to join even before authentication is complete.

Usage: This indicates that the local BP has received an EAP-Success before authentication has even been completed.

Examples: For device-id AP_00-0A-F5-00-01-89 , the upstream AP 00:0a:f5:00:06:22 with SSID NewYorkRm authenticating via local BP radio 0 sent EAP-Success before authentication completed : IT MIGHT BE A ROGUE AP

See Also:

Security: Profile not configured for user-group

Notification which indicates that the AP has determined that a STA is a member of group for which a corresponding service profile has NOT been configured in this SSID.

Syntax: "For device-id %s, the STA %s on radio %d with user %s is in group %s but SSID %s has no profile configured for that group"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
User	User ID
Group	Group tag for this user (determined from RADIUS configuration)
SSID	Identifies the SSID on this AP that the STA has associated with.

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated during Station authentication when no service profile has been configured for a given Group.

Usage: This indicates that the AP has detected a STA is authenticating which is a member of a group for which no service profile has yet been configured in this SSID.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc on radio 0 with user paul is in group employee but SSID NewYorkRm has no profile configured for that group.

See Also:

Security: STA has failed security enforcement check

Notification which indicates that the AP has determined that a STA has failed the security enforcement checks for its service profile.

Syntax: "For device-id %s, the STA %s on radio %d with user %s and SSID %s of group %s failed the security enforcement check with auth-type %d and enc-type %d at enforcement level %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID
SSID	Identifies the SSID on this AP that the STA has associated with.
Group	Group tag for this user (determined from RADIUS configuration)
Authentication Type	The valid types include: NONE (0), SHARED KEY (1), LEGACY EAP (2), RSN PSK (3), RSN EAP (4)
Encryption Type	The valid types include: NONE (0), WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)
Enforcement Level	The security enforcement level configured in the service profile: AES ONLY (1) TKIP OR AES (2), WEP ONLY (3), NO ENCRYPTION (4), DEFAULT ENFORCEMENT (5)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated if the STA fails the security enforcement checks for its service profile

Usage: This indicates that the STA is attempting to use an encryption type that is not allowed in its service profile. The service profile is determined based on the SSID and user group of the STA. Note that the AP may advertize multiple encryption capabilities, but different STAs might be restricted to different subsets of encryption capabilities based on their service profiles.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:cc on radio 0 with user paul and SSID NewYorkRm of group employee failed the security enforcement check with auth-type 4 and enc-type 5 at enforcement level 1

See Also:

Security: Guest Authentication Succeeded

Notification which indicates that a “Guest Access” Station has been successfully authenticated

Syntax: "For device-id %s , Guest authentication succeeded for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which is generated when a “Guest Station” is authenticated.

Usage: This indicates the successful start of a “Guest Access” Stations communications session. This Guest STA will be offered the communications services specified in the Guest Profilethat has been configured for the specified SSID.

Examples: For device-id AP_00-0A-F5-00-01-89 , Guest authentication succeeded for STA 00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and guest mode 4

See Also: Security: Guest Authentication Failed

Security: Guest Authentication Failed

Notification which indicates that a “Guest Access” Station has failed authentication

Syntax: "For device id %s, Guest authentication failed for STA %s on radio %d with SSID %s using captive portal %s and guest mode %d due to %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
----------	-------------------------------

Station	MAC address of the Guest STAtion.
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the Guest has associated with.
Captive Portal	Identifies the “Landing Page” that has accomplished authentication of the Guest STA. This is either simply the Internal “Landing Page”, or a URL identifying the “External Landing Page” which performed the authentication.
Guest Mode	Currently, always set to 4.
Reason code	Currently, always set to 0.

Alarm Severity

Severity	Critical
----------	----------

Description: Notification which is generated when a “Guest Station” fails authentication.

Usage: This indicates that a Guest Station did not present the appropriate “credentials” (currently simple password) upon request.

Examples: For device-id AP_00-0A-F5-00-01-89 , Guest authentication failed for STA 00:0a:f5:00:05:f0 on radio 0 with SSID NewYorkRoom using captive portal Internal and guest mode 4 due to 0

See Also: `Security: Guest Authentication Succeeded`

Security: AP Detected Bad TKIP MIC

Notification which indicates that the AP has detected a BAD TKIP MIC value in an incoming frame encrypted with the pairwise/uniastr key.

Syntax: "For device-id %s, a bad TKIP MIC was detected on an incoming unicast packet from STA %s on radio %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when a bad TKIP MIC is detected on an incoming frame from a STA that is encrypted with the pairwise/unicast key.

Usage: This indicates that the AP has detected an invalid TKIP MIC value on an incoming

frame. All packets received by the AP are always encrypted with the pairwise/unicast key.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected on an incoming unicast packet from STA 00:0a:f5:00:05:cc on radio 0

See Also:

Security: BP Detected Bad TKIP MIC on Incoming Unicast

Notification which indicates that the BP has detected a BAD TKIP MIC value in an incoming frame from the AP that is encrypted with the pairwise/unicast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an incoming unicast packet from the AP %s"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
AP MAC address	The MAC address of the source AP

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.

Usage: This indicates that the BP has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming unicast packet from the AP 00:0a:f5:00:06:22

See Also: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Security: BP Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Notification which indicates that the BP has detected a BAD TKIP MIC value in an incoming frame from the AP that is encrypted with the group/multicast/broadcast key.

Syntax: "For device-id %s, a bad TKIP MIC was detected by local BP radio %d on an incoming multicast/broadcast packet from the AP %s"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Radio	Identifies Radio by interface ID on the Access Point
AP MAC address	The MAC address of the source AP

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when a bad TKIP MIC is detected by a local BP radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/multicast/broadcast key..
- Usage:** This indicates that the BP has detected an invalid TKIP MIC value on a received multicast/broadcast frame.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by local BP radio 0 on an incoming multicast/broadcast packet from the AP 00:0a:f5:00:06:22
- See Also:** BP Detected Bad TKIP MIC on Incoming Unicast

Security: STA Detected Bad TKIP MIC on Incoming Unicast

Notification which indicates that a STA associated with this AP has detected a BAD TKIP MIC value in a frame it received from the AP encrypted with the pairwise/unicast key.

- Syntax:** "For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming unicast packet from the AP"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when a bad TKIP MIC is detected by an STA associated with this AP on an incoming unicast packet from the AP, where the packet is encrypted with the pairwise/unicast key.
- Usage:** This indicates that the STA has detected an invalid TKIP MIC value on an incoming frame encrypted with the pairwise/unicast key.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA 00:0a:f5:00:05:f0 on radio 0 on an incoming unicast packet from the AP

See Also: STA Deteted Bad TKIP MIC on Incoming Multicast/Broadcast

Security: STA Detected Bad TKIP MIC on Incoming Multicast/Broadcast

Notification which indicates that a STA associated with this AP has detected a BAD TKIP MIC value in a multicast/broadcast frame it received from the AP.

Syntax: "For device-id %s, a bad TKIP MIC was detected by STA %s on radio %d on an incoming multicast/broadcast packet from the AP"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
Radio	Identifies Radio by interface ID on the Access Point

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when a bad TKIP MIC is detected by an STA associated with a radio, identified by aniApRadioIndex, on an incoming multicast or broadcast packet from the AP where the packet is encrypted with the group/multicast/broadcast key.

Usage: This indicates that the STA has detected an invalid TKIP MIC value on a received, multicast, frame.

Examples: For device-id AP_00-0A-F5-00-01-89 , a bad TKIP MIC was detected by STA 00:0a:f5:00:05:f0 on radio 0 on an incoming multicast/broadcast packet from the AP

See Also: STA Detected Bad TKIP MIC on Incoming Unicast

Security: TKIP counter-measures lockout period started

Notification which indicates that the AP is taking active counter-measures against an attempted compromise of TKIP.

Syntax: "For device-id %s, the TKIP counter-measures lockout period has started for 60 seconds."

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
----------	-------------------------------

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when a TKIP counter measures lockout period for 60 seconds is started.
- Usage:** This 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 STAs and prevents new STAs from associating for a period of 60 seconds.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the TKIP counter-measures lockout period has started for 60 seconds.

See Also:

Security: EAP User-ID timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with its User-ID during the authentication exchange.

- Syntax:** "For device-id %s, the STA %s[%d] on radio %d and SSID %s did not send its user-id in time to complete its auth sequence with auth-type %d and enc-type %d."

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: LEGACY 8021.x (2), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when an STA fails to send its user-id in time to complete its authentication sequence using the specified authentication type.
- Usage:** This indicates the failure of a STA to complete the EAP authentication exchange in a timely fashion. The two authentication modes that require the STA to send its user-id are WPA EAP and legacy 8021.x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 and SSID NewYorkRm did not send its user-id in time to complete its auth sequence with auth-type 4 and enc-type 6

See Also: EAP Response Timeout, STA Authentication Timeout

Security: EAP response timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with an EAP response during the authentication exchange.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send an EAP-Response in time to complete its auth sequence with auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	Supplicant User ID established during EAPOL Authentication exchange
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: LEGACY 802.1x (2), WPA EAP (4)
Encryption Type	The valid types include: WEP-64 (1), WEP-128 (2), TKIP (5), AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when an STA fails to send an EAP-Response in time to complete its authentication sequence using the specified authentication type and encryption. This is an EAP response other than the User-ID.

Usage: This indicates the failure of a STA to complete its EAP authentication exchange in a timely fashion. The two authentication modes that require the STA to send EAP responses are WPA EAP and legacy 802.1x for dynamic WEP. This trap might indicate that a user prompt is not attended to on the client side. It may also indicate that the client silently rejected a EAP request sent from the RADIUS server – perhaps because it did not trust the RADIUS server’s credentials.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send an EAP-Response in time to complete its auth sequence with auth-type 4 and enc-type 6

See Also: EAP User-ID Timeout, STA Authentication Timeout

Security: EAPOL Key exchange – message 2 timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL 4-way handshake message number 2.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #2 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicabe)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when an STA fails to send the WPA EAPOL-Key Pairwise Message #2 in time to complete the pairwise key exchange.

Usage: This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #2 in time where auth-type 4 and enc-type 6

See Also:

Security: EAPOL Key exchange – message 4 timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL 4-way handshake message number 4.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include:WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)

Alarm Severity

Severity	Critical
----------	----------

Description: This notification is generated when an STA 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.

Usage: This indicates the failure of a STA to complete the EAPOL 4-way key exchange in a timely fashion.

Examples: For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Pairwise Messg #4 in time where auth-type 4 and enc-type 6

See Also:

Security: EAPOL Group 2 key exchange timeout

Notification which indicates that the STA has failed to respond, in a timely manner, with EAPOL Group key exchange message number 2.

Syntax: "For device-id %s, the STA %s[%d] on radio %d with user %s and SSID %s did not send the WPA EAPOL-Key Group Messg #2 in time where auth-

type %d and enc-type %d"

Alarm Parameters

DeviceId	The Device ID of the Airgo AP
Station	MAC address of the Station.
bpIndicator	Identifies if the supplicant is a BP (1), or a STA (0).
Radio	Identifies Radio by interface ID on the Access Point
User	User ID established during EAPOL Authentication exchange (if applicable)
SSID	Identifies the SSID on this AP that the STA has associated with.
Authentication type	The valid types include: WPA PSK (3), WPA EAP (4)
Encryption Type	The valid types include: TKIP (5), AES (6)

Alarm Severity

Severity	Critical
----------	----------

- Description:** This notification is generated when an STA 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.
- Usage:** This indicates the failure of a STA to complete the Group Key exchange in a timely fashion.
- Examples:** For device-id AP_00-0A-F5-00-01-89 , the STA 00:0a:f5:00:05:f0 [0] on radio 0 with user paul and SSID NewYorkRm did not send the WPA EAPOL-Key Group Messg #2 in time where auth-type 4 and enc-type 6

See Also:

Glossary

This glossary defines terms that apply to wireless and networking technology in general and Airgo products in particular.

802.1x

Standard for port-based authentication in LANs. Identifies each users and allows connectivity based on policies in a centrally managed server.

802.11

Refers to the set of WLAN standards developed by IEEE. The three commonly in use today are 802.11a, 802.11b, and 802.11g, sometimes referred to collectively as Dot11.

Access Control List (ACL)

A list of services used for security of programs and operating systems. Lists users and groups together with the access awarded for each.

Access Point (AP)

An inter-networking device that connects wired and wireless networks together. Also, an 802.11x capable device that may support one or more 802.11 network interfaces in it and co-ordinates clients stations in establishing an Extended Service Set 802.11 network

Advanced Encryption Standard (AES)

An encryption algorithm developed for use by U.S. Government agencies and now incorporated into encryption standards for commercial transactions.

Airgo Client Utility (ACU)

Application that executes on a client station and provides management and diagnostics functionality for the 802.11 network interfaces.

Ad-Hoc network

A group of nodes or systems communicating with each other without an intervening Access Point. Many wireless network cards support ad-hoc networking modes.

Authentication Server

A central resources that verifies the identity of prospective network users and grants access based on pre-defined policies.

Authentication Zone

A administrative grouping of resources for user authentication.

Backhaul

The process of getting data from a source and sending it for distribution over the main backbone network. Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Also referred to a WDS.x.

Basic Service Set (BSS)

The set of all wireless client stations controlled by a single access point. The BSSID, or identifier, for the basic service set can be assigned or default to the MAC address of the access point.

Bridge

A connection between two (or more) LANs using the same protocol. Virtual bridges are used as a means of defining layer 2 domains for broadcast messages. Each virtual bridge uniquely defines a virtual local area network (VLAN).

Class of Service (COS)

A method of specifying and grouping applications into various QoS groups or categories.

Differentiated Services Code Point (DSCP)

A system of assigning Quality of Service “Class of Service” tags.

Domain Name Service (DNS)

A standard methodology for converting alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

A communications protocol enabling IP address assignments to be managed both dynamically and centrally. With DHCP enabled on a node (a system, device, network card, or Access Point), when it boots or is connected to a network, an address is automatically assigned. Each assigned address is considered to be “leased” to a specific node; when the lease expires, a new IP can be requested and/or automatically reassigned. Without DHCP, IP addresses would need to be entered manually for each and every device on the network.

Dynamic Frequency Selection (DFS)

A method for selecting the least intrusive and noisy available frequency for operation, part of the 802.11 specification.

Dynamic IP Address

A TCP/IP network address assigned temporarily (or dynamically) by a central server, also known as a DHCP server. A node set to accept dynamic IPs is said to be a “DHCP client.”

Extensible Authentication Protocol (EAP)

Standard that specifies the method of communication between an authentication server and the client, or supplicant, requesting access to the network. EAP supports a variety of authentication methods.

Extensible Authentication Protocol Over LAN (EAPOL)

Protocol used for 802.1x authentication.

EAP-TLS

EAP using Transport Layer Security. EAP-based authentication method based on X.509 certificates, which provides mutual, secure authentication. Certificates must be maintained in the authentication server and supplicant.

EAP-PEAP

Protected EAP-based authentication method based on X.509 certificates. Uses a two-phase approach in which the server is first authenticated to the supplicant.

This establishes a secure channel over which the supplicant can be authenticated to the server.

Extended Service Set (ESS)

A set of multiple connected BSSs. From the perspective of network clients, the ESS functions as one wireless network, with clients able to roam between the BSSs within the ESS.

ESSID

Name or identifier of the ESS used in network configuration.

hostname

The unique, fully qualified name assigned to a network computer, providing an alternative to the IP address as a way to identify the computer for networking purposes.

Hypertext Transfer Protocol (HTTP)

Protocol governing the transfer of data on the World Wide Web between servers and browser (and browser enabled software applications).

Hypertext Transfer Protocol over SSL (HTTPS)

A variant of HTTP that uses SSL (Secure Sockets Layer) encryption to secure data transmissions. HTTPS uses port 443, as opposed to HTTP which uses port 80.

Independent Basic Service Set (IBSS)

A set of clients communicating with each other or a network via an Access Point.

Internet Protocol (IP)

The network layer protocol for routing packets through the Internet.

IP address

32-bit number, usually presented as a period-separated (dotted decimal) list of three-digit numbers, which identifies an entity on the Internet according to the Internet Protocol standard.

Local Area Network (LAN)

A group of computers, servers, printers, and other devices connected to one another, with the ability to share data between them.

Maskbits

Number of bits in the subnet prefix for an IP address, (provides the same information as subnet mask). Each triplet of digits in an IP address consists of 8 bits. To specify the subnet in maskbits, count the number of bits in the prefix. To specify using a subnet mask, indicate the masked bits as an IP address. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Media Access Control (MAC) Address

A unique hardware-based equipment identifier, set during device manufacture. The MAC address uniquely identifies each node of a network. Access Points can be configured with MAC access lists, allowing only certain specific devices to connect with the LAN through them, or to allow certain MAC-identified network cards or devices access only to certain resources.

MAC address authentication

Method of authenticating clients by using the MAC address of the client station as opposed to the user.

Network Address Translation (NAT)

The translation of one IP address used within a network to another address used elsewhere. One frequent use of NAT is the translation of IPs used *inside* a company, versus the IP addresses visible to the outside world. This feature helps increase network security to a small degree, because when the address is translated, this provides an opportunity to authenticate the request and/or to match it to known, authorized types of requests. NAT is also used sometimes to map multiple nodes to a single outwardly visible IP address.

Network Interface Card (NIC)

Generic term for network interface hardware that includes wired and wireless LAN adapter cards, PC Cardbus PCMCIA cards, and USB-to-LAN adapters.

Network Management System (NMS)

Software application that controls a network of multiple access points and clients.

Node

Generic term for a network entity. Includes a access point, network adapter (wireless or wired), or network appliance (such as a print server or other non-computer device)

Network Time Protocol (NTP)

NTP servers are used to synchronize clocks on computers and other devices. Airgo APs have the capability to connect automatically to NTP servers to set their own clocks on a regular basis.

Ping Packet INternet Groper (ping)

A utility which determines whether a specific IP address is accessible, and the amount of network time (measured in milliseconds) for response. Ping is used primarily to troubleshoot Internet connections.

Policy-based Networking

The management of a network with rules (or policies), governing the priority and availability of bandwidth and resources, based both on the type of data being transmitted, as well as the privileges assigned to a given user or group of users. This allows network administrators to control how the network is used, to help maximize efficiency.

Power Over Ethernet (PoE)

Power supplied to a device by way of the Ethernet network data cable instead of a electrical power cord.

Preamble Type

The preamble defines the length of the cyclic redundancy check (CRC) block for communication between the Access Point and a roaming network adapter. All nodes on a given network should use the same preamble type.

Quality of Service (QoS)

QoS is a term encompassing the management of network performance, based on the notion that transmission speed, signal integrity, and error rates can be managed,

measured, and improved. In a wireless network, QoS is commonly managed through the use of policies.

Remote Authentication Dial-In User Service (RADIUS)

A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize service or system access. RADIUS permits maintenance of user profiles in a central repository that all remote servers can share.

Radio Frequency (RF)

The electromagnetic wave frequency radio used for communications applications.

Roaming

Analogous to the way cellular phone roaming works, roaming in the wireless networking environment is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Rogue AP

An access point that connects to the wireless network without authorization.

Secure SHell (SSH)

Also known as the Secure Socket Shell, SSH is a UNIX-based command line interface for secure access to remote systems. Both ends of communication are secured and authenticated using a digital certificate, and any passwords exchanged are encrypted.

Service Set Identifier (SSID)

The SSID is a unique identifier attached to all packets sent over a wireless network, identifying one or more wireless network adapters as “belonging” to a common group. Some Access Points can support multiple SSIDs, allowing for varying privileges and capabilities, based on user roles.

Secure Sockets Layer (SSL)

A common protocol for message transmission security on the Internet. Existing as a program layer between Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP)

Protocol used to transfer email messages between email servers.

Simple Network Management Protocol (SNMP)

An efficient protocol for network management and device monitoring.

SNMP trap

A process that filters SNMP messages and saves or drops them, depending upon how the system is configured.

Spanning Tree Protocol (STP)

A protocol that prevents bridging loops from forming due to incorrectly configured networks.

Station (STA)

An 802.11 capable device that supports only one 802.11 network interface, capable of establishing a Basic Service Set 802.11 network (i.e., peer-to-peer network)

Static IP Address

A permanent IP address assigned to a node in a TCP/IP network.

Subnet

Portion of a network, designated by a particular set of IP addresses. Provides a hierarchy for addressing in LANs. Also called subnetwork.

Subnet Mask

A TCP/IP addressing method for dividing IP-based networks into subgroups or subnets (compare with maskbits). Each triplet of digits in an IP address consists of 8 bits. To specify using a subnet mask, indicate the masked bits as an IP address. To specify the subnet in maskbits, count the number of bits in the prefix. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Temporal Key Integrity Protocol (TKIP)

Part of the IEEE 802.11i encryption standard. TKIP provides improvements to WEP encryption, including per-packet key mixing, message integrity check and a re-keying mechanism.

Traffic Class Identifier (TCID)

Part of the standard 802.11 frame header. The 3-bit TCID is used for mapping to class-of-service values.

Transmission Control Protocol/Internet Protocol (TCP/IP)

One of the most commonly used communication protocols in modern networking. Addresses used in TCP/IP usually consist of four triplets of digits, plus a subnet mask (for example, 192.168.25.3, subnet 255.255.255.0).

Transport Layer Security (TLS)

Protocol that provides privacy protection for applications that communicate with each other and their users on the Internet. TLS is a successor to the Secure Sockets Layer (SSL).

Trunk

In telecommunications, a communications channel between two switching systems. In a wireless network, a trunk is a wireless connection from one access point to another.

Type of Service (ToS)

Sometimes also called IP Precedence, ToS is a system of applying QoS methodologies, based on headers placed into transmitted IP packets.

User Datagram Protocol (UDP)

A connectionless protocol similar to TCP/IP, but without the same level of error-checking. UDP is commonly used when some small degree of errors and packet-loss can be tolerated without losing program integrity, such as for online games.

Virtual LAN (VLAN)

A local area network with a definition that addresses network nodes on some basis other than physical location or even whether the systems are wired together or operating using the same local equipment. VLANs are, on average, much easier to manage than a physically implemented LAN. In other words, moving a user from one VLAN to another is a simple change in software, whereas on a regular LAN, the computer or device would need to be connected physically to a different switch

Index

Numerics

- 128-bit encryption 137
- 64-bit encryption 137
- 802.11
 - 802.11a,802.11b,802.11g 7
 - definition 275
 - extensions 69
 - mode in 2.4 GHz band 69
 - policy configuration 69
- 802.11i 12
- 802.1p 7
- 802.1Q 7
- 802.1x 5, 12, 136, 275

A

- access control list (ACL) 275
- access point
 - introduction 1
 - placement 27
 - rebooting 209
 - rogue 173
- access point (AP) 1
 - beacon name 131
 - components 25
 - configuration management 214
 - definition 275
 - enrollment 165
 - hostname 33
 - interfaces 99
 - mode, selecting 62
 - name in beacon 58
- accessing
 - NM Portal 45, 164
 - the AP 30
- ack mode 67
- activating DHCP server 189
- add to discovery database 183
- address resolution protocol (ARP)
table 102
- ad-hoc network 275
- admin
 - state 62
- administrative users 205
- administrator 144
 - authentication 145
 - email address 36
 - password 36, 145
 - security 144
- administrator security 135
- admission 68
 - backhaul criteria 68
 - multi vendor criteria 68
- advanced
 - radio configuration 69
 - RADIUS parameters 150
- advanced encryption standard (AES) 12
 - definition 275
 - statistics 90
 - with WPA 139
- alarm
 - count 193
 - filter 201
 - ID 193
 - panel 37
 - summary 192, 193
 - table 192, 193
- alarms
 - list and description 233
 - logging time 193
 - total 193
- AP hostname 33
- AP security 135
- assigning IP address to interface 122
- association
 - status 87
 - type 87
- association status 88
- association type 88
- asterisk next to field name 30
- authentication 5
 - diagnostics 146, 149
 - server 141, 275
 - timeout 150
 - type 87
 - user 12, 136
 - zones 143
- authentication zone 275
 - task overview 14
- authorization state 170
- auto/manual 170
- auto-discovery
 - configuration 182, 184

- automatic channel selection 65
- automatically generated password 154, 158
- auto-select channel 58
- auto-sync database 186
- auxiliary manager 213

B

- background scanning 58
- backhaul 127, 275
 - admission criteria 68
 - AP and BP radios 128
 - applications 127
 - authentication 127
 - candidate APs 131
 - link criteria 129
 - security 128
 - trunk 128, 131
 - uplink criteria 130
 - viewing topology 168
- backhaul point (BP) 55
 - mode, selecting 62
- backup 214, 218
- backup restore portal databases 188
- band 65
- basic rate set 70
- basic service set (BSS) 276
- beacon
 - name 58, 131
 - period 72
- bootstrap
 - NM Portal 164
 - password 136
 - policy 180
 - security mode 35
- bootstrapping
 - the AP 31
- br1 101
- br4094 101
- branch office installation 16
- bridge
 - definition 276
 - details table 101
 - forwarding table 101
 - prefix 101

- statistics 102
- bridge and STP tab 100
- bridging services 100
- broadcast SSID in beacon 81
- BSS type 172
- BSSID 276
- BSSID criteria 130
- burst ack 69
- buzzer 213, 214
- byte statistics 88

C

- cabling requirements 26
- campus installation 16
- candidate APs 131
- captive portal 153
- cell size and range management 3
- certificate 204
- channel
 - ID 169
 - set 65
- channel configuration 35, 41, 64
- channel list 65
- channel management 3
- choosing access point locations 25
- class 172
- class of service (COS) 6, 82, 111, 112, 276
 - class order 116
 - levels 111
 - overview 6
 - priority settings 6
- class order 112
- client LAN adapter 1
- client stations, managing 86
- Client Utility 275
- clock 43
- command conventions xi
- command line interface (CLI) 8, 227
 - getting help 228
- common problems and solutions 224
- compatibility status 77
- configuration
 - reset 217
 - syslog 211
- configuration interfaces 30
- configuration reports 215
- configuring 129
 - bridging services 100
 - DHCP server 188
 - interfaces 121
 - network discovery 182
 - packet filters 119

- portals 185
- quality of service 111
- RADIUS parameters 150
- SNMP 123
- VLANs 105
- console port 228
 - connection 25
 - settings 228
- conventions, command xi
- COS
 - levels 114
- COS MAC layer mapping 6
- COS to IP mappings 6
- COS-to-TCID 114
- country code 41, 58
- coverage and capacity requirements 10

D

- data encryption 5, 137
 - overview 12
- data rates supported 7
- date setting 34, 42
- default
 - gateway 33
 - SSID 78
 - VLAN 105
 - assigned to interface 107
- default gateway 34
- defer threshold 69
- delivery traffic indication message (DTIM) 72
- deployment environment 41, 58
- destination
 - AP 169
 - radio 169
- detection time 172
- device ID 136, 167, 170
- DHCP server
 - activating 189
 - configuring 188
- diagnostics
 - authentication 149
- differentiated services code point (DSCP) 117, 276
- diffServ code point (DSCP)-to-COS mapping 112
- disassociating a station 88
- discovered radios 171
- discovery 182
 - interval 182
 - method 172
 - scope 184

- seed 184
- discovery configuration
 - scope/seed 183
- DNS 33
- DNS IP address 210
- domain name service (DNS) 276
 - and guest access 153
- dot11 QoS 66, 68
- downlink statistics 88
- downloading software 219
- dynamic frequency selection (DFS) 276
- dynamic host configuration protocol (DHCP) 33, 276
 - IP address 210
 - lease 191
- dynamic IP address 276

E

- EAP-PEAP 137, 276
- EAP-TLS 137, 276
- egress COS 112, 114
- encapsulation configuration 122
- encryption type 87
- enhanced
 - data rates 7, 66, 68
 - rate set 69
- enrolling APs 165
- enrollment 12, 136
 - overview 12
 - portal 4
 - server 136
- ESSID 277
- eth0 99
- example 9
- extended service set (ESS) 277
- extensible authentication protocol (EAP) 136, 276
- external landing page 53, 155
- external RADIUS server 141
- external RADIUS server settings 145

F

- factory defaults 217
 - resetting
 - radio 62
- fault management 192
 - alarm summary 192
- field asterisk 30
- filter
 - alarm 201
 - statistics 121
 - table 119

filters 119
 fragmentation threshold 72
 FUNK-RADIUS 5

G

gateway IP address 210
 generating bootstrap policy 180
 global radio configuration 57
 graph
 link test 95
 group key
 retries 150
 group name 87
 guest access 153
 and VLANs 157
 and wireless security 156
 configuring 156
 external landing page 53
 internal landing page 51
 overview 6
 panel 158
 security 160
 shared secret 53
 task overview 15
 URL 53
 VLAN 53
 wizard 50
 guest access security 135
 guest password 154, 158
 guest service profile 157
 guest table 158
 guest VLAN 157

H

hardware options 213
 HCF 69
 help, command line interface 228
 highest node priority 130
 Home 164
 home panel 37
 hostname 33, 277
 https 136
 https download 221
 hypermode 66, 68
 hypertext transfer protocol
 (HTTP) 277
 hypertext transfer protocol over SSL
 (HTTPS) 277

I

IAPP
 service 91
 statistics 92

 topology 91
 ICMP ping 125
 IEEE802.1x 136
 independent basic service set
 (IBSS) 277
 ingress QoS 112, 113
 initializing
 normal AP 33
 portal AP 36
 installation
 planning 9
 requirements 25
 scenarios 16
 installing the AP 26
 integration with existing network 7
 inter access point protocol (IAPP) 90
 interdependencies
 channel configuration 67
 global radio 63
 interface
 statistics 123
 tab 107
 table 122
 interfaces 99
 configuring 121
 interface-to-COS mapping 111
 internal landing page 51, 154
 internet protocol (IP) 277
 IP address 277
 assigning to interface 122
 link for AP 168
 of AP 33
 IP configuration 210
 IP Precedence tab 119
 IP precedence-to-COS mapping 112
 IP Protocol tab 118
 IP protocol-to-COS mapping 112
 IP rogue discovery 173
 IP routing 6
 configuration 103
 IP subnet criteria 130
 IP topology 169
 IP-DSCP tab 117

L

landing page 153
 external 155
 internal 154
 large office installation 16
 lease time 189
 LEDs 28
 levels 6
 license key 214

license management 212
 link
 statistics 88
 link criteria 129
 link test 94
 adding 95
 graph 95
 load balancing 69
 local area network (LAN) 277
 logging in to the web interface 31
 logging module name 195
 logical interfaces 99
 long retry limit 72
 lowest hop count 130
 lowest weighted cost 130

M

MAC address 87, 170
 configuration 71
 MAC address authentication 278
 MAC-ACL users 206
 management
 interface options 8
 VLAN 105
 management information base
 (MIB) 123
 management IP address 210
 management VLAN 106
 managing
 faults 192
 users 203
 maskbits 277
 maximum number of leases 189
 media access control (MAC)
 address 277
 menu tree 37, 164
 Microsoft-IAS 5
 mid-size office installation 16
 mobility management 3
 model number 44
 multi domain support 41, 58
 multiple SSIDs 78, 85
 multiple VLANs 5

N

navigating the web interface 37
 neighbors 171
 network
 connectivity parameters 58
 default settings 99
 density 58
 discovery 182
 information requirements 26

- management 12, 163
- radio neighbors 171
- topology 165
- network address translation (NAT) 278
- network density 34
- network interface card (NIC) 278
- network management system (NMS) 278
- network time protocol (NTP) 278
- networking services 99
- NM Explorer Home panel 164
- NM Portal 4, 163
 - access 45
 - features 163
 - initializing 36
- NM services 179
- NMS configuration 212
- NMS Professional 1
- NMS-Professional 2, 163
 - interface options 8
- no authentication security 137
- node 278
- normal AP 127
- NTP server 189

O

- open
 - access 140
 - encryption 137
- open security
 - quick start option 35
- operating bands 35, 41
- operational state 170
- overview 6

P

- packet filters 119
- password
 - administrator 145
 - AP 167
- password authentication procedure (PAP) 145
- path selection criteria 130
- performance configuration 66, 68
- persona 62
- ping packet internet groper (ping) 278
- ping test 125
- planning your installation 9
- policy
 - bootstrapping 180
 - defining 180
 - table 179

- policy management 179
- policy-based networking 278
- port number 143
- portal
 - architecture 4
 - configuration 185
 - database backup/restore 188
 - database version 186
 - secure backup 187
 - services 170
 - services overview 4
 - table 186
- portal AP
 - initializing 36
- power over Ethernet (PoE) 27, 278
- power requirements 26
- preamble type 278
- primary manager 213
- problems and solutions 224
- product features 2
- product suite 1
- profile table 84
- protocols, data rates, and coverage 10

Q

- quality of service (QoS) 6, 111, 278
 - advanced features 115
 - class order 112, 116
 - features 111
 - statistics 115
 - task overview 15
 - user group-based 6
- Quick Start 31
 - panels 39

R

- radio
 - advanced configuration 69
 - channel configuration 64
 - configuration panel 56
 - diagnostics 93
 - discovered 171
 - interface 35, 41
 - neighbors 77, 171
 - state 72
 - statistics 72, 75
- radio frequency (RF) 279
- radio resource management 3
- RADIUS 141, 150
 - authentication zones 143
 - group attribute 150
 - server 143
 - server settings 145

- with backhaul 127
- rate adaptation 66, 68
- real time clock (RTC) 214
- real-time clock 213
- rebooting the AP 209
- receiver rate adaptation 69
- redundant security portal 186
- regulatory and license information 231
- remote authentication dial-in user service (RADIUS) 136, 279
- remote MAC address 131
- reporting AP 172
- reports
 - configuration 215
- required field 30
- reset
 - configuration 217
 - subsystems 217
 - to default 217
 - to factory defaults 217
- resetting
 - AP 29
 - to factory defaults 29
- resetting radio 62
- restore 188, 214, 218
- re-trunk count 169
- re-trunking 128
- retry limits 72
- retry statistics 88
- roaming 279
- rogue AP 173, 279
 - features 6
 - management overview 6
 - reasons 173
 - unclassified 173, 176
- rogue AP discovery
 - IP 173
 - wireless 173
- RTS threshold 72

S

- scope/seed 183
- secure backup
 - NM Portal 187
- secure shell (SSH) 227, 279
- secure sockets layer (SSL) 279
- security 144
 - administrator 135
 - and guest access 160
 - AP 135
 - backhaul 128
 - certificate 204

- data encryption 12
 - enforcement 82
 - enrollment 12
 - features 5
 - guest access 135
 - mode 138
 - overview 11
 - statistics 88, 146
 - user 135
 - wireless 138
 - security portal 4
 - enrolling 167
 - redundant 186
 - seed 183
 - selecting method 12
 - serial number 44
 - service profile 79
 - add or modify 85
 - bind to SSID 79
 - change binding 83
 - guest 157
 - SSID binding 83
 - task overview 15
 - service set identifier (SSID) 279
 - and service profiles 79
 - broadcast in beacon 81
 - details 82
 - information 80
 - max stations 80
 - multiple SSIDs 85
 - name 34
 - service type attribute 145
 - shared secret 143
 - for guest access 53
 - short retry limit 72
 - signal quality 172
 - signal strength 172
 - simple mail transfer protocol (SMTP) 279
 - community 124
 - server 36
 - trap 124
 - simple network management protocol (SNMP) 123, 136, 279
 - site surveys 11
 - small office installation 16
 - SMTP server address 43
 - SNMP trap 279
 - software
 - upgrade 219
 - software distribution
 - cancelling 223
 - software distribution process 222
 - software download status 223
 - software image file 220
 - software image recovery 224
 - source
 - AP name 169
 - radio 169
 - spanning tree protocol (STP) 100, 101, 279
 - SSH 136
 - SSID
 - authentication 140
 - binding to service profile 83
 - configuring 78
 - criteria 130
 - default 78
 - example 78
 - multiple 6
 - STA 279
 - standards supported 7
 - start discovery 183
 - static
 - IP address 280
 - station 279
 - link statistics 88
 - MAC address 88
 - management 86
 - statistics
 - supplicant 147
 - subnet 280
 - subnet mask 280
 - supplicant statistics 146, 147
 - supported standards and data rates 7
 - syslog
 - configuration 211
 - viewing 202
 - system configuration
 - managing 209
 - system determined band 65
 - system requirements 25
- ## T
- tagged VLAN 106
 - task roadmaps 14
 - Telnet 25
 - temporal key integrity protocol (TKIP) 139, 280
 - TFTP download 222
 - TFTP server 214, 218
 - thumbprint 136, 167, 170
 - time
 - discovered 170
 - setting 34, 42
 - zone setting 34, 42
 - timeout statistics 88
 - traffic class identifier (TCID) 280
 - traffic class identifiers (TCID) 111
 - transmission control protocol/internet protocol (TCP/IP) 280
 - transport layer security (TLS) 280
 - trap 124
 - trunk 128, 280
 - statistics 132
 - table 131
 - type of service (ToS) 280
- ## U
- unauthenticated users 153
 - unclassified rogue AP 173, 176
 - unenroll an AP 168
 - upgrading AP software 220
 - upgrading software 219
 - uplink
 - configuration 130
 - statistics 88
 - URL
 - for guest access 53
 - user
 - authentication 12, 136
 - group 15, 82
 - name 87
 - VLAN 108
 - user datagram protocol (UDP) 280
 - user security 135
 - user security wizard 45
 - open access 46, 49
 - WEP 46, 48
 - WPA-EAP 46
 - WPA-PSK 46, 47
 - users
 - adding administrative users 205
 - adding MAC-ACL users 206
 - managing 203
 - unauthenticated 153
 - wireless 203
 - using NM Portal 164
- ## V
- vendor specific attribute 145
 - verifying AP installation 28
 - version table 44
 - virtual LAN (VLAN) 280
 - VLAN 82
 - 4094 101
 - and guest access 5
 - example 105
 - guest 157

- guest access 53
- ID 106, 108
- interface 5
- name 106
- overview 5
- statistics 110
- table 106
- tag 106
- task overview 15, 20, 22
- user 5, 108
- VLANs
 - multiple 5
- VLAN-to-COS mapping 111
- W**
- walk test 97
 - parameters 97
- web browser
 - interface 8, 30
 - navigating the interface 37
- web interface 8
- Wi-Fi 280
- wi-fi protected access (WPA) 5, 12
 - quick start option 35
- Windows internet name server (WINS) 280
- wired equivalent privacy (WEP) 5, 12, 137, 280
 - key 35
 - keys 140
 - quick start options 35
 - security 140
 - statistics 90
- wireless
 - network 9
 - security 138
 - users 203
- wireless backhaul 127, 129
 - AP and BP radios 128
 - applications 127
 - candidate APs 131
 - link criteria 129
 - security 128
 - trunk 128
 - trunks 131
 - uplink criteria 130
 - viewing topology 168
- wireless LAN adapter 1
- wireless local area network (WLAN) 280
- wireless rogue discovery 173
- wizard
 - guest access 50
 - user security 45
- wlan0, wlan1 99
- world mode 65
 - country code 41, 58
 - multi domain support 41, 58
- WPA security 139
- WPA-AES 137
- WPA-EAP 139
- WPA-PSK 137, 139
- WPA-PSK passphrase 35
- WPA-TKIP 137