

HP M330 Dual Radio 802.11ac Access Point Configuration and Administration Guide



HP Part Number: 5998-6740
Published: March 2015
Edition: 1

© Copyright 2015 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

Microsoft® and Windows® are U.S. trademarks of the Microsoft group of companies. Google Chrome™ browser is a trademark of Google Inc.

Warranty

WARRANTY STATEMENT: See the warranty information sheet provided in the product box and available online.

Supported Access Point Models

This document applies to these M330 models:

- JLO62A HP M330 Dual Radio 802.11ac (AM) AP
- JLO63A HP M330 Dual Radio 802.11ac (WW) AP
- JLO64A HP M330 Dual Radio 802.11ac (JP) AP

Contents

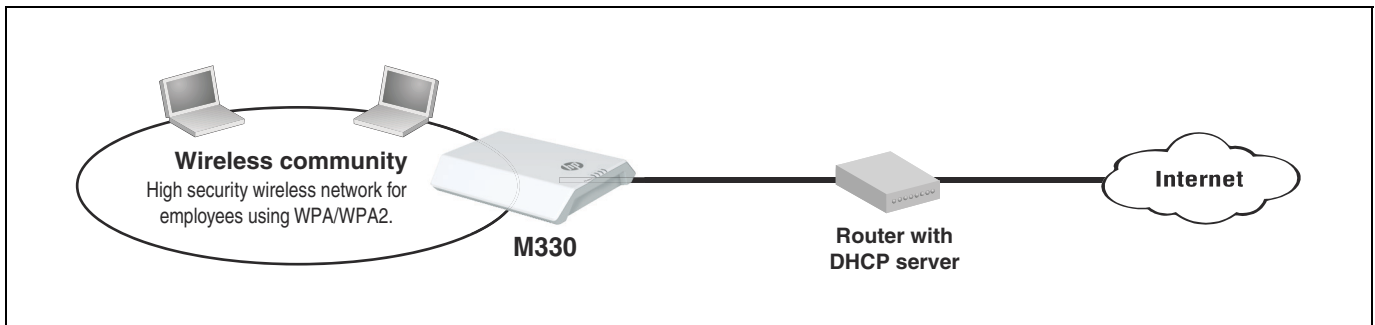
1 Deploying the M330	7
2 Using Quick setup	9
Overview	9
Automatically running Quick setup the first time you log in	9
Accessing Quick Setup after your first log in	12
Quick Setup wizard	12
Step 1: Specify access point settings	13
Step 2: Specify access point cluster settings	14
Step 3: Specify wireless network settings	14
System summary	17
3 Managing the M330	19
Configuring web server settings	19
Web server configuration	19
Administrator login credentials	20
SSH configuration	20
Telnet configuration	21
Scheduler	21
Scheduler association	23
SNMP configuration	24
Supported MIBs	25
System time	26
Set system time	26
Daylight saving	27
4 Working with wireless communities and authentication	29
Overview	29
Configuring global RADIUS servers	29
Managing wireless communities	31
About the default wireless community	31
Wireless community configuration options	32
Wireless protection	33
MAC authentication	40
5 Wireless configuration	43
Wireless coverage	43
Factors limiting wireless coverage	43
Configuring overlapping wireless APs	44
802.11ac and 802.11n best practices	48
Supporting legacy wireless clients	48
Channel width	50
Radio configuration	51
Country	51
Basic settings	51
Advanced radio settings	54
Load balancing	57
Detecting rogue APs	58
Enabling scanning	58
Detected and known AP lists	58
Working with saved AP lists	60
Viewing wireless information	60
Viewing all connected wireless clients	60

Viewing wireless statistics for the radio	62
6 Creating WDS links	65
Key concepts	65
Simultaneous AP and WDS support	65
Using the 5 GHz band for WDS links	66
Configuration considerations	66
WDS configuration	67
Example of a WDS Deployment	69
General Information	69
Setting up a WDS link	69
Multiple WDS link configuration	73
General Information	73
Setting up multiple WDS links	73
7 Configuring Ethernet, IP, and VLAN settings	77
Ethernet configuration	77
IPv4 configuration	78
Automatically assigning an IP address (default method)	78
Static IP configuration	78
IPv6 configuration	79
VLAN configuration	80
VLAN assignment via wireless communities	80
VLAN assignment via RADIUS	81
Port statistics	83
8 Clustering multiple M330s	85
Overview	85
Shared settings in a cluster	85
IPv4 and IPv6 clusters	87
Cluster formation	87
Client connections	89
Channel planning	90
Stopping/Starting Automatic Channel Assignment	90
Configuration	91
Current channel assignments	91
9 Captive portal	93
Overview	93
Setting-up captive portal	94
Basic configuration	95
Advanced configuration	96
Creating a captive portal instance	96
Configuring a captive portal instance	97
Community binding	100
Web customization	101
Creating a web locale	101
Customizing a web locale	102
Previewing a web locale	106
Local user/group association	106
Creating local captive portal groups	107
Creating local captive portal users	107
Client list	108
Example of guest captive portal configuration	110
Initial settings	110
Basic configuration	110
Advanced configuration	111
Community binding	112

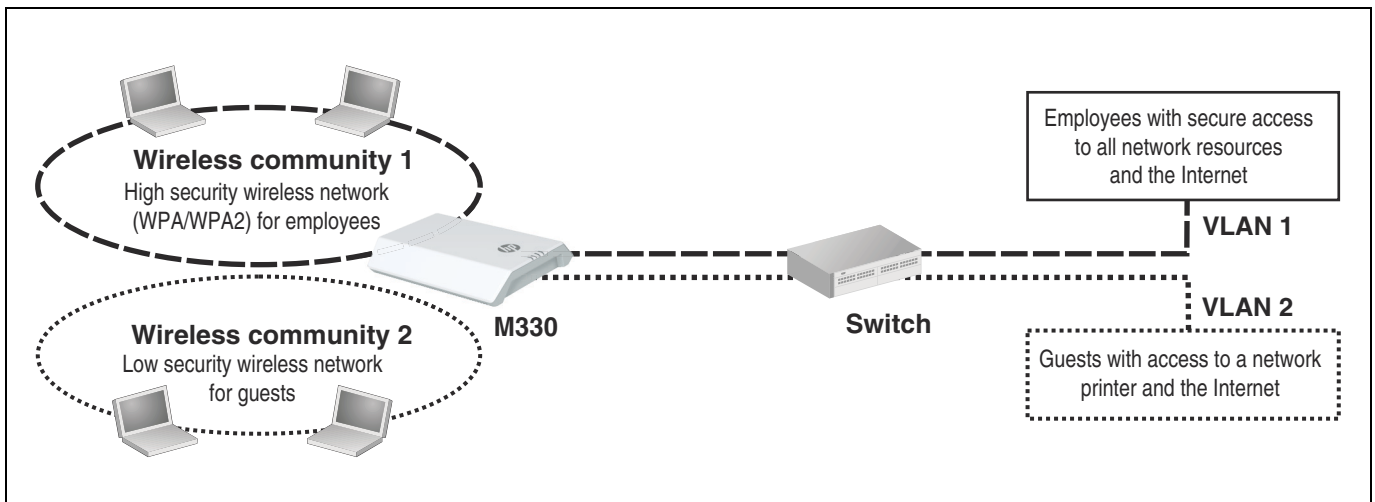
Web customization	112
Test captive portal client access	114
10 Maintenance.....	117
Configuration file management	117
Reset.....	117
Save	117
Restore	118
Reboot	118
Software updates.....	118
Software information	119
Switching the software image	119
Software upgrade.....	119
System information	119
Viewing the EULA	120
11 Tools.....	121
System log	121
System log configuration.....	121
Remote syslog configuration	122
Events	123
Email alert	123
General configuration	123
Mail server configuration	125
Message configuration	125
Sending a test message	126
Viewing email alert status	126
Network trace configuration	127
Overview.....	127
Packet trace configuration	127
Packet file trace	128
Remote packet trace.....	129
Packet trace status.....	131
Packet trace file download	132
Ping	133
12 Support and other resources	135
Online documentation	135
Contacting HP	135
HP websites	135
Conventions	136
A Resetting to factory defaults	137
Factory reset procedures	137
Using the reset button.....	137
Using the management tool	137

1 Deploying the M330

In a small office, the M330 can be directly connected to a broadband router (DSL or cable) to provide wireless networking for all employees. In the following scenario, employees can share data and resources with each other and access the Internet at the same time:



With its wireless community feature, the M330 can be configured to provide up to eight separate wireless networks (all on the same wireless channel), each with its own configuration settings for security, VLAN support, and more.



In this scenario, employees connect to wireless community 1, which is protected with WPA/WPA2. All employee traffic exits the M330 on VLAN 1, providing access to private resources on the company network and on the Internet.

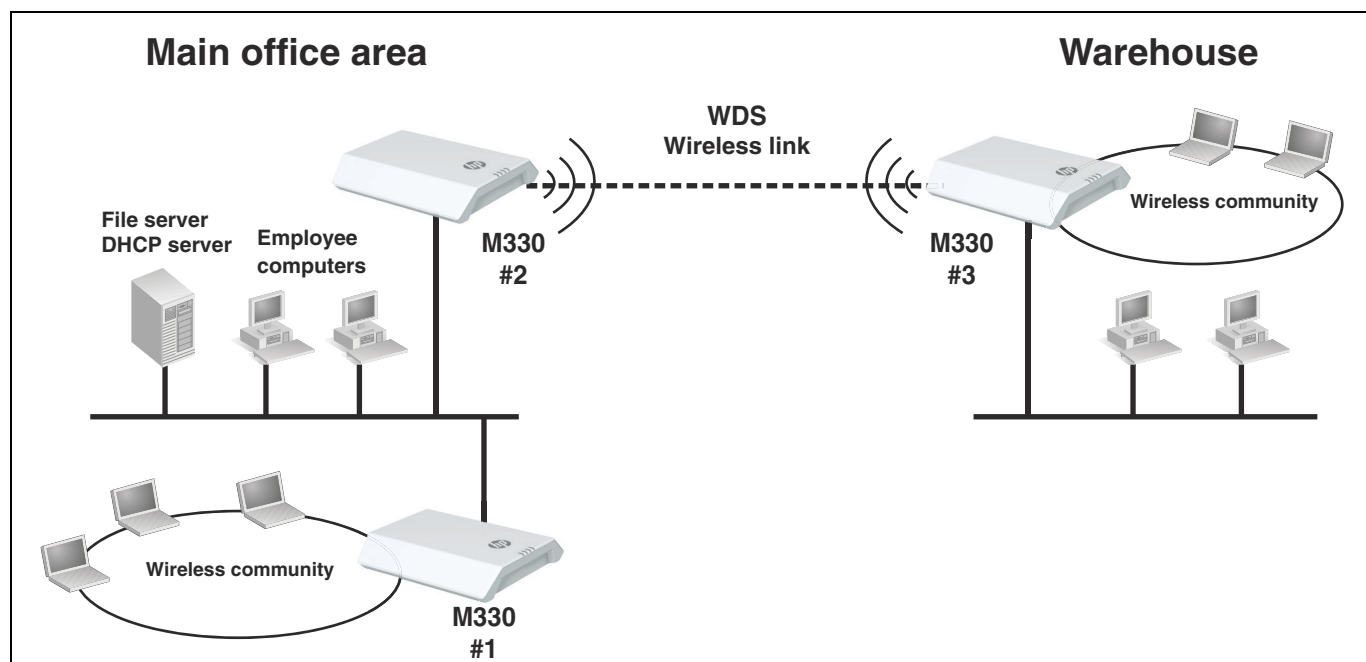
Guests connect to wireless community 2, which is protected with WEP. All guest traffic exits the M330 on VLAN 2, providing access only to the Internet.

Note

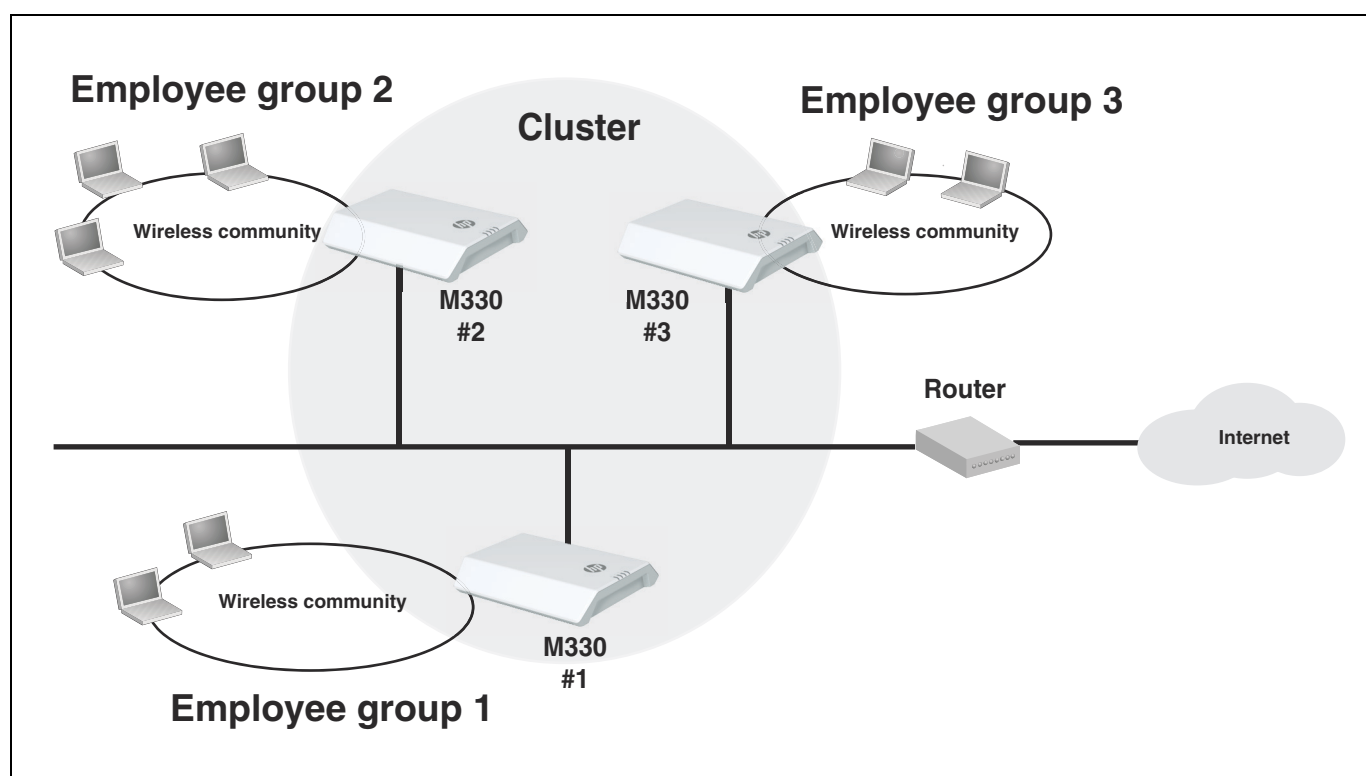
WEP is available only when the radio mode does not support 802.11n.

For offices that already have a wired networking infrastructure, the M330 is easily integrated to provide wireless networking. It can also be used to extend the reach of the network to areas that are difficult or impossible to reach with traditional cabling.

In the following scenario, M330 #1 provides wireless network services to the employees in the main office, while M330 #2 and M330 #3 use the Wireless Distribution System (WDS) to create a wireless link between the main office network and a small network in a warehouse. WDS eliminates the need to run cabling, allowing for fast and easy deployment.



In the following scenario, three M330s provide distinct employee groups access to the Internet through a router on the network. The M330s are joined in a cluster, which enables them to share a single configuration and to be administered as a single unit. Channel planning may be implemented on the cluster to reduce interference and optimize wireless bandwidth usage.



2 Using Quick setup

Overview

Quick setup provides an easy way to quickly configure settings on the M330 for several different networking scenarios. Just pick the scenario that most closely resembles your installation and fill in the appropriate fields.

Automatically running Quick setup the first time you log in

The first time you log in to the management tool (see the *HP M330 Dual Radio 802.11ac Access Point Quick Start Guide* for first time login procedure), the HP end user license agreement displays. When you accept the agreement, a page displays to enable you to select your country so that wireless radio settings are configured appropriately. Select **Save** to display the first page in the Quick setup wizard.

This page lets you choose one of five configuration scenarios to use as the basis for your setup, as described in the following sections.

Basic wireless network

Choose this option if you want to create a single wireless network to provide wireless connectivity for your users. This option can be used to connect the M330 directly to a broadband router or to an existing wired network, using static IP, DHCP, or IPv6 addressing.

This scenario supports clustering mode, where multiple APs in the network are deployed and administered as a single entity.

Quickly setup the M330

Quick setup can help you to configure the M330 for several different networking environments. Select the option that most closely matches your needs and then click OK.

☒ Recommend wireless network settings based upon your network environment

Network Environment Basic wireless network

☐ Manually configure wireless network settings

Save **Cancel**

Multiple wireless networks

Choose this option if you want to create multiple wireless networks to support users with different networking requirements. For example, you could create two wireless networks, one for employees and one for guests.

This option can be used to connect the M330 to a network using static IP, DHCP, or IPv6 addressing. This scenario also supports clustering mode, where multiple APs in the network are deployed and administered as a single entity.

Quickly setup the M330

Quick setup can help you to configure the M330 for several different networking environments. Select the option that most closely matches your needs and then click OK.

☒ Recommend wireless network settings based upon your network environment

Network Environment Multiple wireless networks

Wireless community 1
High security wireless network for employees using WPA/WPA2.

Wireless community 2
Low security wireless network for guests.

M330
providing 802.11a/b/g/n/ac wireless services

Router with DHCP server

Internet

☐ Manually configure wireless network settings

Save Cancel

Multiple wireless networks with wired VLANs

Choose this option if you want to:

- Create multiple wireless networks to support users with different requirements.
- Map the traffic from each wireless network to a specific VLAN.

As in Multiple wireless networks mode, this option supports static IP, DHCP, or IPv6 addressing for the network connection, and supports clustering mode.

Quickly setup the M330

Quick setup can help you to configure the M330 for several different networking environments
Select the option that most closely matches your needs and then click OK

☒ Recommend wireless network settings based upon your network environment

Network Environment Multiple wireless networks with wired VLANs

Wireless community 1
High security wireless network for employees using WPA/WPA2.

Wireless community 2
Low security wireless network for guests.

M330 providing 802.11a/b/g/n/ac wireless services

Switch

VLAN 1
Employees with secure access to all network resources and the Internet.

VLAN 2
Guests with access to a network printer and the Internet.

☐ Manually configure wireless network settings

Save **Cancel**

Multiple wireless networks with RADIUS authentication

Choose this option if you want to:

- Create multiple wireless networks to support users with different requirements.
- Map the traffic from each wireless network to a specific VLAN.
- Authenticate user login credentials using a third-party RADIUS server.

This option can be used to connect the M330 to a network using static IP, DHCP, or IPv6 addressing. This scenario also supports clustering mode, where multiple APs in the network are deployed and administered as a single entity.

Quickly setup the M330

Quick setup can help you to configure the M330 for several different networking environments
Select the option that most closely matches your needs and then click OK

☒ Recommend wireless network settings based upon your network environment

Network Environment Multiple wireless networks with RADIUS authentication

Wireless community 1
High security wireless network (802.1X or WPA) for employees.

Wireless community 2
Low security wireless network for guests.

M330 providing 802.11a/b/g/n/ac wireless services

Switch

VLAN 1
Employees with secure access to all network resources and the Internet.

VLAN 2
Guests with access to a network printer and the Internet.

RADIUS server

Authentication

☐ Manually configure wireless network settings

Save **Cancel**

Add to wireless network with existing AP cluster

Use this option if your network already has a defined cluster of M330 APs and you want this AP to join the cluster.

Quickly setup the M330

Quick setup can help you to configure the M330 for several different networking environments. Select the option that most closely matches your needs and then click OK.

☒ Recommend wireless network settings based upon your network environment

Network Environment: Add to wireless network with existing AP cluster

Wireless community 1
High security wireless network for employees using WPA/WPA2.

Wireless community 2
Low security wireless network for guests.

M330
providing 802.11a/b/g/n/ac wireless services

Router with DHCP server

Internet

☐ Manually configure wireless network settings

Save **Cancel**

Accessing Quick Setup after your first log in

When you log in subsequent to completing or cancelling out of the Quick Setup wizard, the System Summary page displays by default. You can view and configure the Quick Setup settings by selecting **Home > Quick Setup**.

See also the *HP M330 Dual Radio 802.11ac Access Point Quick Start Guide*, which describes the configuration procedure for a basic wireless network.

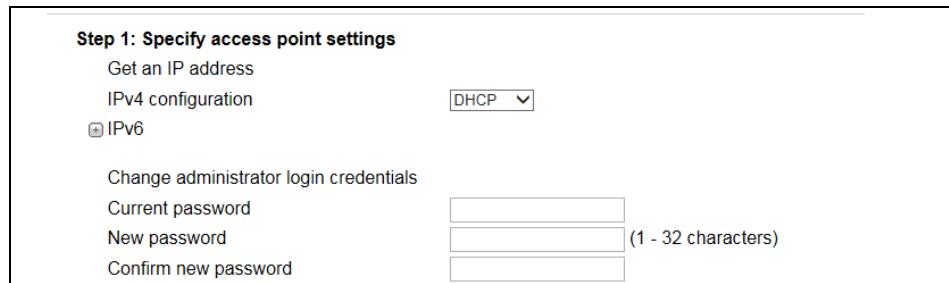
Quick Setup wizard

To use the Quick Setup wizard, select one of the following options for the network environment, as described in the previous sections, and click **Save**:

- “Basic wireless network” on page 9
- “Multiple wireless networks” on page 10
- “Multiple wireless networks with wired VLANs” on page 10
- “Multiple wireless networks with RADIUS authentication” on page 11
- “Add to wireless network with existing AP cluster” on page 12

Step 1: Specify access point settings

For a complete description of all settings, see the relevant section.



Step 1: Specify access point settings

Get an IP address

IPv4 configuration DHCP ▼

+ IPv6

Change administrator login credentials

Current password

New password (1 - 32 characters)

Confirm new password

Get an IP address

You can use these settings to configure IP addresses and how they are assigned. The **IPv4 configuration** field displays by default. To configure IPv6 settings, click the + symbol to the left of **IPv6**.

You can configure addresses for both protocol versions. Only IPv4 supports DHCP.

For more information on setting an IPv4 address, see [“IPv4 configuration” on page 78](#).

For more information on setting an IPv6 address, see [“IPv6 configuration” on page 79](#).

Change administrator login credentials

The M330 supports one administrator login with a default username and password **admin**. Use this section to change the password.

Note

As an immediate first step in securing your wireless network, HP recommends that you change the administrator password from the default.

For more information on setting the administrator password, see [“Administrator login credentials” on page 20](#).

Configure system settings

When you configure the Quick Setup settings by selecting **Home > Quick Setup**, the system settings are also displayed.

In the Configure system settings area, you can specify a name and location that helps identify the M330. You can also specify a person to contact for administrative purposes.

The **System name** appears in the banner at the top of the M330 web management tool interface.

Step 2: Specify access point cluster settings

Use this section to configure whether this AP functions as a member of a cluster of APs on the network.

To add the M330 to a cluster, set **Clustering** to **Enabled**, specify a **Cluster name** (the same name must be used for all members of the cluster), optionally specify a **Cluster location**, and set the **Cluster IP version** to either **IPv4** or **IPv6**.

Step 2: Specify access point cluster settings
Configure access point clustering
Clustering ☐ Enable ☒ Disable
Cluster name
Cluster location
Clustering IP version ☒ IPv4 ☐ IPv6

For more information on clustering, see [“Clustering multiple M330s” on page 85](#).

Note

If the selected network environment was **Add to wireless network with existing AP cluster**, the Quick setup wizard is complete. Select **Save** to have the AP join the cluster.

Step 3: Specify wireless network settings

Use this section to define wireless networks and to configure the security settings for client access and encryption.

This section displays different settings, depending on the selected network environment.

Step 3: Specify wireless network settings
Radio
Wireless mode

	Network name (SSID)	VLAN ID	Security	Delete
0	<input type="text" value="HP1_2.4G"/>	<input type="text" value="1"/>	WPA personal	

= SSID Off = SSID On = SSID On and configured for broadcast

[Add New Wireless Community](#)

Wireless community settings
Identify the wireless network
Network name (SSID)
Map wireless network to a VLAN
VLAN ID (1 - 4094)
Secure the wireless network
Security method
WPA versions ☐ WPA (TKIP) ☒ WPA2 (AES)
Protected management frames ☐ Disabled ☒ Supported ☐ Mandatory
Key (8 - 63 characters)
Confirm key

[Update](#) [Cancel](#)

[Save](#) [Cancel](#)

Configure the radio and wireless mode

Select a radio to configure. Select **Radio 1** (2.4 GHz band) for 802.11b/g/n modes, or **Radio 2** (5 GHz band) for 802.11ac and 802.11n modes.

Select the mode that best supports the wireless clients at your location.

For more information on setting the **Wireless mode**, see [“Radio configuration” on page 51](#).

Wireless community settings

The M330 allows you to create up to eight wireless communities. Each wireless community defines the settings for a distinct wireless network, with its own network name (SSID), settings for wireless protection, user authentication, VLANs, and more. Radio settings are shared by all wireless communities.

Default wireless communities are defined on the M330. The name (or SSID) for the 2.4 GHz radio is **HP1_2.4G** and the 5 GHz radio is **HP1_5G**. Both are assigned to VLAN 1. The settings that initially display in the Wireless community settings pertain to the default communities.

Note

Before creating a new community, ensure that the name (SSID), VLAN, and security settings for the default community are configured as needed.

For more information on wireless communities, see [“Managing wireless communities” on page 31](#).

For more information on mapping a wireless community to a VLAN, see [“VLAN configuration” on page 80](#).

Secure the wireless network

A security method (or no security method) can be associated with the default wireless community and any additional communities you create. The available security methods and selected default settings vary depending on the selected network environment. The following table lists the security options available with each environment.

Note

You can also disable security on each wireless community. However, this is not recommended.

Network environment	Security methods
Basic	If the wireless mode includes 802.11n:
Multiple wireless networks	<ul style="list-style-type: none">WPA/WPA2 Personal (default)
Multiple wireless networks with wired VLANs	If the wireless mode does not include 802.11n: <ul style="list-style-type: none">Static WEP (see note)WPA/WPA2 Personal (default)

Network environment	Security methods
Multiple wireless networks with RADIUS authentication	<p>If the wireless mode includes 802.11 n:</p> <ul style="list-style-type: none"> • WPA/WPA2 Personal • WPA/WPA2 Enterprise (default) <p>If the wireless mode does not include 802.11 n:</p> <ul style="list-style-type: none"> • Static WEP (see note) • 802.1X/Dynamic WEP (see note) • WPA/WPA2 Personal • WPA/WPA2 Enterprise (default)
Add to wireless network with existing AP cluster	The AP will inherit its security settings from the cluster.
Note: WEP-based security is not available in 802.11 n modes due to Wi-Fi security requirements.	

For more information on wireless security, see [“Wireless protection” on page 33](#).

After you select a security method and complete the related settings, the Quick setup wizard is complete.

System summary

After you complete the Quick setup wizard, when you log into the management tool again, the System Summary page displays.

System Summary	
System information	
IP address	192.168.1.1
Static IPv6 address	
IPv6 autoconfigured global addresses	
IPv6 link local address	fe80::2a80:23ff:fe99:6230/64
MAC address	28:80:23:99:62:30
Firmware version	V0.0.0.39-M330-B000-0
Product identifier	JL062A
Hardware version	R0B
Serial number	CN4ZGV8051
Device description	HP M330 Wireless 802.11ac Access Point
Country	US - United States
Wireless	
Radio 1	
Status	Enable
Mode	IEEE 802.11b/g/n
Channel	1 (2412 MHz)
Operational bandwidth	20
Radio 2	
Status	Enable
Mode	IEEE 802.11a/n/ac
Channel	132 (5660 MHz)
Operational bandwidth	80
Refresh	

System information

This page includes the following system information:

- **IP address:** The IP address assigned to the AP. See the *Network > IP* page to configure IP information.
- **Static IPv6 address:** The IPv6 address assigned to the AP, if one is configured.
- **IPv6 autoconfigured global addresses:** The global IPv6 address, if one or more has been assigned automatically using the network prefix that is sent by routers in router advertisements.
- **IPv6 link local address:** The link local address is derived automatically using the prefix fe80::/64 and the MAC address of the AP.
- **MAC address:** The MAC address of the AP. This is the address by which the AP is known externally to other networks.

This MAC address applies to the Ethernet port on the AP and to the first (default) wireless community, referred to as wlan0. The MAC address is incremented by 1 for each additional wireless community that you create. For example, if the Ethernet and wlan0 interfaces are assigned MAC address 00:55:9A:3C:7A:00, then the next wireless community you create will be assigned MAC address 00:55:9A:3C:7A:01, and so on.

- **Firmware version:** The version of firmware installed on the AP.
- **Product identifier:** The AP hardware model ID number.
- **Hardware version:** The AP hardware version.
- **Serial number:** The AP serial number.
- **Device description:** Information about the product hardware.
- **Country:** The configured country of operation, also known as the regulatory domain.

Wireless

This page also includes the following radio (1 and 2) information:

- **Status:** The AP radio current operating status.
- **Mode:** The AP radio current operating mode.
- **Channel:** The AP radio current operating channel.
- **Operational Bandwidth:** The AP radio current operating channel bandwidth.

3 Managing the M330

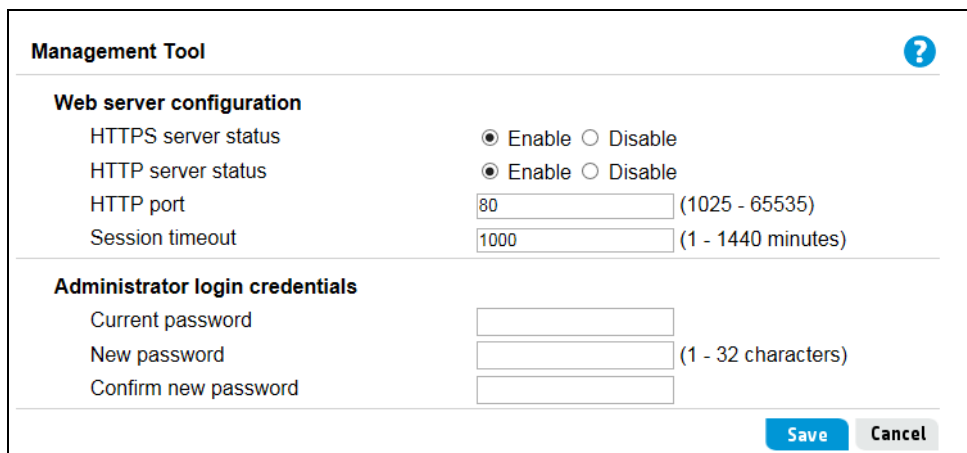
The M330 is managed via its web-based management tool using Microsoft Internet Explorer 8 or later, Google Chrome V29, or Mozilla Firefox V24 or later. You can access the M330 management tool using either **http** or **https**. Using **https** is more secure, but you will see a warning because the security certificate is issued by the M330 and not a known certificate authority. With **https**, it is acceptable to choose the option that allows you to proceed through the security warning.

In a web browser, specify either: **http://192.168.1.1** or **https://192.168.1.1**.

For information on launching the management tool for the first time, see the *HP M330 Dual Radio 802.11ac Access Point Quick Start Guide*.

Configuring web server settings

Select **Management** > **Management tool** to configure web server settings.



The screenshot shows the 'Management Tool' configuration page. It has a title bar with a question mark icon. The page is divided into two main sections: 'Web server configuration' and 'Administrator login credentials'. In the 'Web server configuration' section, there are four settings: 'HTTPS server status' and 'HTTP server status', both with 'Enable' selected; 'HTTP port' with a value of 80; and 'Session timeout' with a value of 1000. The 'Administrator login credentials' section has three input fields for 'Current password', 'New password', and 'Confirm new password'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Management Tool	
Web server configuration	
HTTPS server status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTP server status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTP port	<input type="text" value="80"/> (1025 - 65535)
Session timeout	<input type="text" value="1000"/> (1 - 1440 minutes)
Administrator login credentials	
Current password	<input type="password"/>
New password	<input type="password"/> (1 - 32 characters)
Confirm new password	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Web server configuration

Use this section to configure web access to the management tool.

[HTTPS server status](#)

[HTTP server status](#)

The M330 software includes HTTP and HTTPS functionality to enable communication with your web browser. Unlike HTTP, HTTPS enables secure sessions, using a digital certificate to encrypt data exchanged between the M330 and your web browser. HTTP and HTTPS are both enabled by default.

Note

If you disable the protocol you are currently using to access the management interface and click Save, the current connection is terminated and you cannot access the AP using that protocol until it is enabled.

HTTP port

By default, the HTTP server uses the well-known logical port number 80 for communication with clients. You can specify a different port number if port 80 is blocked or used for a different protocol on your network.

Session timeout

If there is no activity on the management session for the specified time, the administrator will be automatically logged off. Specify a time in the range 1-1440 minutes. The default is 5 minutes.

Administrator login credentials

The M330 supports one administrator login account. Use the following settings to change the password.

Note

As an immediate first step in securing your wireless network, HP strongly recommends that you change the administrator password from the default.

Current password

The default password is **admin**.

New password and Confirm password

Specify a new password for the M330 administrator account.

The administrator password can be from 1 to 32 alphanumeric characters. Do not use special characters or spaces. For security purposes, HP recommends that the password be at least 6 characters.

Caution

If you forget the administrator password, the only way to access the administrator account is to reset the M330 to factory default settings. See [“Factory reset procedures” on page 137](#).

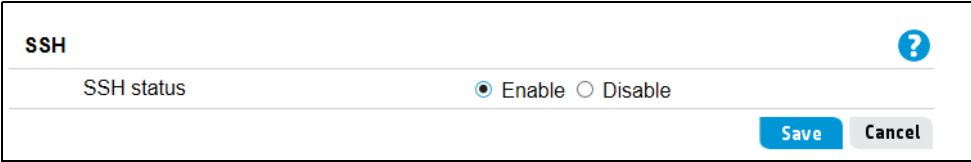
SSH configuration

For advanced network management, Secure Shell (SSH) is a remote management tool that can be used to access the M330's command-line interface (CLI) from anywhere in the network. SSH acts as a secure replacement for Telnet, using generated public keys to encrypt all data passing between the M330 and an SSH-enabled management station. An administrator can securely use a user name and password for authentication and management access to the M330.

Note

SSH client software needs to be installed on the management station to access the M330 for management using the SSH protocol.

Select **Management > SSH** to configure SSH settings.



SSH	
SSH status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<div>Save Cancel</div>	

Select to enable or disable SSH access to the CLI. SSH access is enabled by default.

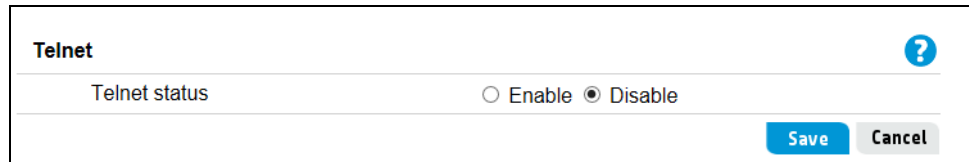
Telnet configuration

Telnet is a remote management tool that can be used to access the M330's command-line interface (CLI) from anywhere in the network. Note that Telnet is not completely secure from hostile attacks, HP recommends that SSH be used as a secure replacement for Telnet.

Note

Telnet client software needs to be installed on the management station to access the M330 for management using Telnet.

Select **Management > Telnet** to configure Telnet settings.



Select to enable or disable Telnet access to the CLI. Telnet access is disabled by default.

Scheduler

The Scheduler enables radio and wireless community (VSC) interfaces to be enabled or disabled at specified times. This feature can be used to automatically enable radios only during office hours, or to disable VSCs at times for improved security or just to reduce power consumption.

Schedule rules can be configured by specifying start and end times for certain days of the week. Each rule is repeated on a weekly basis. A Schedule Profile is constructed by grouping up to 16 non-overlapping schedule rules together. The M330 supports up to 16 schedule profiles that can be associated with a specified radio or VSC.

Select **Management > Scheduler** to configure scheduler settings.

Scheduler

Administrative mode

Status

☐ Enable
☒ Disable

Operational status

Status

Down

Reason

Disabled

Profile configuration

Profile name

(1 - 32 characters)

Add

Rule configuration

Select profile

Set schedule

Start time

:

End time

:

Remove

Add

Profile rule table

Profile name	Occurrence	Start time	End time	Delete
				<div>Modify Rule</div>

Save

Cancel

The following parameters are on the **Scheduler** page.

Administrative mode

Enables or disables the scheduler feature. The default is disabled.

Status

The current operational status of the scheduler, either **up** or **down**.

Reason

Codes that explain the reason for the scheduler status. The following are the possible values:

- **Disabled:** The administrative mode is set to disabled.
- **System time not set:** The M330 system time is not set, either through NTP or manually.
- **Active:** The scheduler is properly configured and enabled.

Profile configuration

Creates a profile to which you can add schedule rules. Enter 1-32 alphanumeric characters. Click **Add** to add the profile name. Up to 16 profile names can be created. By default, there are no profiles.

Rule configuration

Each scheduler profile can have up to 16 schedule rules. The following parameters configure each rule to add to a profile.

- **Select Profile:** Selects the profile to which you want to add rules.
- **Set Schedule:** Sets the day of the week: **Daily**, **Weekday** (Monday to Friday), **Weekend** (Saturday and Sunday), **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**. The default is **Daily**.

- **Start Time:** The time of day to enable a radio or VSC. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.
- **End Time:** The time of day to disable a radio or VSC. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.

Select a configured rule from the table and click **Modify Rule** to change its configuration.

Note

After making any modifications, you must click **Save** to apply the changes and to save the settings.

Scheduler association

The configured schedule profiles must be associated to specific radio and virtual service community (VSC) interfaces to be operational. Only one profile can be associated to a radio or VSC interface, but a single profile can be associated with multiple interfaces. By default, there are no profiles associated to any interfaces.

If a schedule profile associated to a radio or VSC interface is deleted, the interface association is removed automatically. Note that when a radio is disabled, all the VSC interfaces for that radio are also operationally disabled.

After you have associated profiles with radio or VSC interfaces, click **Save** to apply the changes.

Select **Management > Scheduler Association** to configure scheduler association settings.

Scheduler Association

?

Radio		
Radio	Profile name	Operational status
1	<div></div>	up
2	<div></div>	up

Community		
Radio	<div>1</div>	
VSC		
0	<div></div>	up
1	<div></div>	down
2	<div></div>	down
3	<div></div>	down
4	<div></div>	down
5	<div></div>	down
6	<div></div>	down
7	<div></div>	down

Save

Cancel

The following parameters are on the **Scheduler Association** page.

Radio (1/2)

The radio interface for profile association. Radio **1** is the 2.4 GHz band, and **2** is the 5 GHz band.

Radio

Select the radio interface for the VSC profile association.

VSC (0-7)

The virtual service community (wireless community) for profile association.

Profile name

Select the configured profile name to associate to the radio or VSC interface. Only one profile can be selected per interface.

Operational status

The current operational status of the interface.

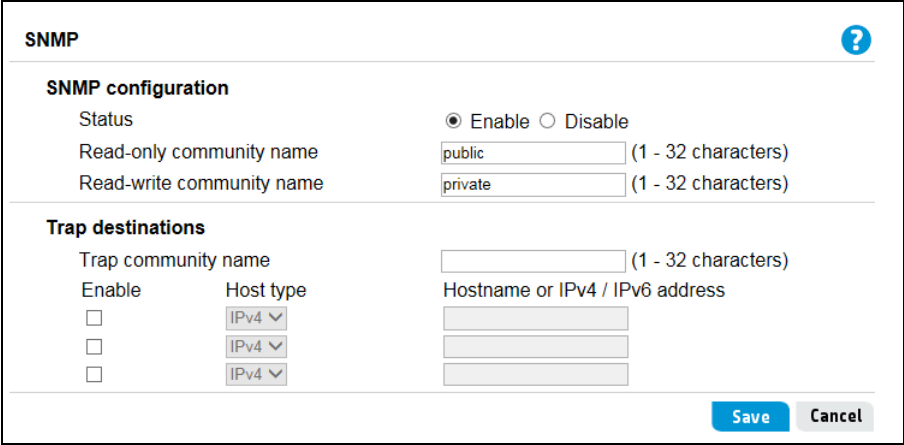
SNMP configuration

The M330 supports Simple Network Management Protocol (SNMP) versions v1 and v2c. The M330 can be enabled to respond to SNMP requests to return information or to set a parameter. The M330 can also be configured to send information to host destinations through trap messages, which informs an administrator that certain events have occurred.

Management access from SNMP v1 or v2c stations is controlled by community names. To communicate with M330, an SNMP v1 or v2c management station must submit a valid community name for authentication.

Select **Management** > **SNMP** to open the SNMP configuration page.

After you have configured the SNMP settings, click **Save** to apply the changes.

A screenshot of the SNMP configuration page. The page has a title bar 'SNMP' with a help icon. Below the title bar is a section 'SNMP configuration'. It contains a 'Status' field with radio buttons for 'Enable' (selected) and 'Disable'. Below that are two text input fields: 'Read-only community name' with the value 'public' and 'Read-write community name' with the value 'private'. Both fields have a note '(1 - 32 characters)'. Below this is a section 'Trap destinations'. It contains a 'Trap community name' text input field with a note '(1 - 32 characters)'. Below that is a table with three columns: 'Enable', 'Host type', and 'Hostname or IPv4 / IPv6 address'. There are three rows, each with an 'Enable' checkbox, a 'Host type' dropdown menu (all set to 'IPv4'), and a 'Hostname or IPv4 / IPv6 address' text input field. At the bottom right of the page are 'Save' and 'Cancel' buttons.

The following parameters are on the **SNMP** page.

Status

Select to enable or disable the SNMP agent. By default, the SNMP agent is enabled. If you disable the agent, the M330 will not respond to SNMP requests.

Read-only community name

This is the password that controls read-only access to SNMP information on the M330. A network management program must supply this name when attempting to get SNMP information from the M330. By default, the name is set to **public**.

Read-write community name

This is the password that controls read-write access to SNMP information on the M330. A network management program must supply this name when attempting to set SNMP parameters on the M330. By default, the name is set to **private**.

Trap community name

To send SNMP trap messages to trap destinations, specify the global community name sent with the traps. The community name can be in any alphanumeric string of 1-32 characters. Special characters are not permitted.

Host type

Specify whether the enabled trap destination host is an IPv4 or an IPv6 address.

Hostname or IPv4/IPv6 address

Enter the DNS hostname or IPv4/IPv6 address of up to three computers to which SNMP traps will be sent. The valid range is 1-256 characters. Be sure to select the Enabled check box next to each hostname.

Supported MIBs

The M330 supports the following standard MIBs:

- BRIDGE-MIB (802.1d)
- ENTITY-MIB (RFC 2737)
- IANAifType-MIB
- IEEE802dot11-MIB
- IF-MIB
- INET-ADDRESS-MIB
- LM-SENSORS-MIB
- RFC1155-SMI
- RFC1212-MIB
- RFC1213-MIB
- RFC1215-MIB
- RFC4668-MIB
- RFC4670-MIB
- IPV6-ICMP-MIB
- IPV6-MIB
- IPV6-TC-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- NET-SNMP-AGENT-MIB
- NET-SNMP-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-VIEW-BASED-ACM-MIB
- SNMP-USER-BASED-SM-MIB
- SNMP-USM-DH-OBJECTS-MIB
- SNMPv2-CONF
- SNMPv2-MIB (RFC 2418)
- SNMPv2-SMI
- SNMPv2-TC
- SNMPv2-TM
- IP-MIB
- TCP-MIB
- UDP-MIB
- UCD-SNMP-MIB
- UCD-DISKIO-MIB
- UCD-DLMOD-MIB
- UCD-IPFILTER-MIB
- UCD-IPFWACC-MIB

System time

The correct system time is important for proper operation of the M330, especially when using the logs to troubleshoot.

Select **Management > System time** to open the System Time page. This page enables you to configure time server and time zone information.

After you have configured the system time settings, click **Save** to apply the changes.

System Time ?

Set system time

System time (24 HR) Tue Jan 1 2013 12:13:31 PST

Set system time ☐ Using network time protocol (NTP) ☒ Manually

System date January 1 2013

System time (24 HR) 12 : 13

Time Zone USA (Pacific)

Adjust time for daylight saving

Enable ☒

DST start (24 HR) Second Sunday in March at 02 : 00

DST end (24 HR) First Sunday in November at 02 : 00

DST offset (minutes) 60

Save Cancel

Set system time

This section displays the current system time. You can configure the time manually or have it automatically configured by a Network Time Protocol (NTP) server.

Manually

Select the date, time (in 24-hour notation), and timezone.

Using network time protocol (NTP)

This option enables the AP to use NTP to synchronize the system clock to global Internet time. NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

When you select the NTP option, a field displays for you to specify the NTP server. You can specify the NTP hostname or IP address, although using the IP address is not recommended, as this is more likely to change.

NTP server address/name

The IP address or name of an NTP server. An actual NTP server host name, **pool.ntp.org**, is configured by default and will provide the time when the AP is connected to the Internet. If you specify a hostname, note the following requirements:

- The length must be from 1 to 253 characters.
- Upper and lower case characters, numbers, and hyphens are accepted.

- The first character must be a letter (a to z or A to Z), and the last character cannot be a hyphen.

Daylight saving

Use this section to enable daylight savings time (DST), if required for your location. The AP automatically sets daylight saving start and end dates based on the time zone selected.

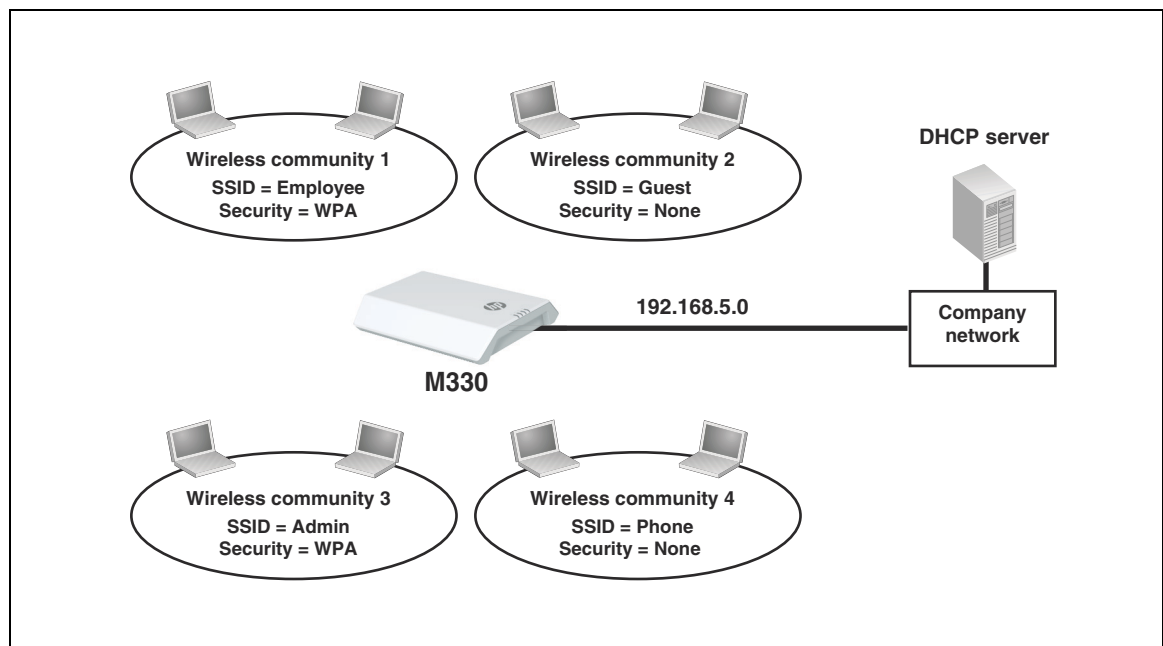
Alternatively, you can manually set the dates for starting and ending the daylight saving. The DST offset specifies how many minutes to move the clock forward or backward.

4 Working with wireless communities and authentication

Overview

The M330 allows you to create up to eight wireless communities (or virtual service communities, VSCs) per radio. Each wireless community defines the settings for a distinct wireless network, with its own network name (SSID), settings for wireless protection, user authentication, VLANs, and more.

For example, in the following scenario, four wireless communities are defined. Each wireless community is configured with a different wireless network name (SSID).



Even though multiple wireless communities are in use, all wireless users are on the same network (192.168.5.0). This means that all wireless users can reach resources on the corporate network. However, communication between wireless users may or may not be possible, depending on the configuration settings defined for each wireless community.

Configuring global RADIUS servers

M330 communities can use third-party RADIUS servers to validate user login credentials for the WPA enterprise, 802.1X, or MAC-based authentication options.

The M330 enables you to define up to four IPv4 and four IPv6 global RADIUS servers, which can be shared by each wireless community.

One server acts as a primary, while the others act as backup servers. The network type (IPv4 or IPv6) and accounting mode are common across all configured global RADIUS servers. After configuring servers, you can select which set to enable (either the IPv4 or the IPv6 servers). You cannot enable a combination of IPv4 and IPv6 servers.

Note

Additional IPv4 or IPv6 RADIUS servers can be configured for each wireless community when 802.1X/Dynamic WEP or WPA-Enterprise is used as the authentication protocol. See [“802.1X/Dynamic WEP” on page 35](#) and [“WPA Enterprise” on page 38](#).

Global RADIUS servers are configured on the **Wireless > Communities** page. Select **+** to the left of **Global RADIUS server settings**.

The screenshot shows the 'Global RADIUS server settings' configuration page. At the top, there is a section header 'Global RADIUS server settings' with a minus icon to its left. Below this, the 'RADIUS IP address type' is set to 'IPv4' (selected with a radio button) and 'IPv6' (unselected). There are four input fields for 'RADIUS IP address', 'RADIUS IP address-1', 'RADIUS IP address-2', and 'RADIUS IP address-3'. Below these are three input fields for 'RADIUS key', 'RADIUS key-1', 'RADIUS key-2', and 'RADIUS key-3'. A note '(1 - 64 characters)' is next to the first key field. At the bottom, there is a checkbox for 'Enable RADIUS accounting' which is currently unchecked.

[RADIUS IP address type](#)

Select **IPv4** or **IPv6** to configure up to four servers of each type. If you configure both types, this selection determines which set of servers is used.

[RADIUS IP address/1/2/3](#)

Enter up to four server IP addresses of the selected type. The first address is the primary RADIUS server. If it is unavailable, the M330 will attempt to use the others in sequence.

[RADIUS key/1/2/3](#)

The RADIUS key is the shared secret key for the global RADIUS server. The first key corresponds to the first IP address, and so on. Enter up to 64 alphanumeric and special characters. The key is case-sensitive, and you must configure the same key on the AP and on your RADIUS server.

Caution

Although you can configure four IPv4 and four IPv6 server IP addresses, you can specify only four keys, which are shared by each set of servers. For example, if you select **IPv4** and specify **RADIUS IP address-2** and the corresponding **RADIUS key-2**, and then select **IPv6**, the **RADIUS key-2** field will retain the previously configured value for use with the IPv6 server. If you specify a new value for the IPv6 configuration, the value in the IPv4 configuration will be updated as well.

[Enable RADIUS accounting](#)

When selected, the RADIUS server will track and measure the resources a particular user has consumed, such as system time, the amount of data transmitted and received, and so on.

Managing wireless communities

To manage wireless communities, select **Wireless > Communities**.

The screenshot shows the 'Communities' configuration page. At the top, there's a 'Radio' dropdown set to '1'. Below it is a table with columns: Network name (SSID), VLAN ID, MAC auth, Security, and Delete. The table contains one entry: HP1_2.4G with VLAN ID 1, MAC auth Disabled, and Security Disabled. Below the table is a legend: 'X = SSID Off', '↑ = SSID On', and '⬇ = SSID On and configured for broadcast'. To the right of the legend is a button 'Add New Wireless Community'. Below this is a form with fields: Network name (SSID) (HP1_2.4G), Broadcast SSID (checked), VLAN ID (1), MAC authentication (Disabled), and Security method (Disabled). At the bottom right of the form are 'Update' and 'Cancel' buttons. At the bottom of the page are 'Save' and 'Cancel' buttons.

Network name (SSID)	VLAN ID	MAC auth	Security	Delete
0 ⬇ HP1_2.4G	1	Disabled	Disabled	

X = SSID Off ↑ = SSID On ⬇ = SSID On and configured for broadcast

Add New Wireless Community

Network name (SSID): HP1_2.4G

Broadcast SSID: ☒

VLAN ID: 1 (1 - 4094)

MAC authentication: Disabled

Security method: Disabled

Update Cancel

Save Cancel

You can define up to eight wireless communities per radio (16 total).

- To edit an existing community, select its name in the list. Settings are displayed for the community selected in the communities list. Modify the settings as needed and select **Update**.
- To add a new community, select **Add New Wireless Community**. You can select **Save** to accept the default settings, or modify the settings and select **Add**, then **Save**.
If you select **Cancel** before selecting **Add**, the new wireless community will be deleted.
If you change these settings after saving a new wireless community, select **Update**, then **Save**. You can select **Cancel** before selecting **Update** to undo any changes to these settings.

See [“Wireless community configuration options” on page 32](#) for details on the settings.

About the default wireless community

By default, a single wireless community is defined for each radio. The name for the 2.4 GHz radio SSID is **HP1_2.4G**, and for the 5 GHz radio **HP1_5G**, which are also the network names (SSIDs). You can modify settings for the default communities, but you cannot delete them. You can create and delete additional communities.

Caution

The default wireless communities do not have any security or authentication options enabled by default. To protect the wireless network from malicious third-party wireless users, HP strongly recommends that you enable some form of wireless protection on the default wireless communities and on other communities you create.

Wireless community configuration options

You can configure the following settings for each wireless community:

Network name (SSID)

Specify a name to uniquely identify the wireless network associated with this community. Each wireless user that wants to connect to this community must use the network name.

By default, the M330 broadcasts this name so that wireless users can see it when they try to connect to the wireless network.

The name is case-sensitive and must include between 2 and 32 alphanumeric characters, including spaces. The following characters are not allowed:

- only spaces
- a space as the first character
- a space as the last character

Broadcast SSID

This option controls whether the network name (SSID) is broadcast to all wireless users.

- When enabled, the wireless network will be visible to wireless clients. Wireless clients are usually configured to automatically discover APs that broadcast their names and connect to the one with the strongest signal.
- When disabled, the network will not be visible to wireless clients. Wireless users must manually specify the network name (SSID) to successfully connect to the network.

VLAN ID

Use this option to set the default VLAN for traffic from this wireless community on the Ethernet port. All traffic sent/received on the Ethernet port by the wireless community will be assigned to this VLAN.

Note

Depending on the security protocol in use for the wireless community, members may be assigned to a VLAN other than the default (the default VLAN ID is 1). Client VLAN assignments from a RADIUS server override the default VLAN assignment.

MAC authentication

This feature enables you to authenticate wireless users based on the MAC addresses of their wireless devices. Select one of the following authentication methods:

- **Disabled:** Do not use MAC authentication.
- **Local:** Use a MAC authentication list that you configure. If you select this option, you must specify a list of allowed or blocked users on the **MAC authentication** page. See [“Local MAC authentication” on page 41](#) for instructions.
- **RADIUS:** Use the MAC authentication list on the external RADIUS server. The M330 uses the RADIUS servers configured for the **Security method** option selected for this wireless community. If no RADIUS servers are defined for the selected security method, the global RADIUS servers are used. See [“RADIUS server-based MAC authentication” on page 40](#).

By default, no global RADIUS server is defined. To define one or more servers, select **Global RADIUS server settings** and configure the **RADIUS IP address type**, **RADIUS IP address**, and **RADIUS key**.

Security method

By default, no security is defined for a wireless community. HP strongly recommends that you configure a security method to provide encrypted data exchanges between wireless clients and the M330. See “Wireless protection” on page 33 for details on the available security methods.

Wireless protection

The M330 provides several methods to protect wireless transmissions from eavesdropping and to safeguard network access by unauthorized users. To choose the method that best meets the needs of your network, refer to the sections that follow.

Static WEP

Static WEP enables you to encrypt wireless transmissions, but does not provide for user authentication. WEP is not as secure as the other security methods available.

Network name (SSID)	VLAN ID	MAC auth	Security	Delete
0 HP1_2.4G	1	Disabled	Disabled	

✖ = SSID Off ⓘ = SSID On ⓘ = SSID On and configured for broadcast

[Add New Wireless Community](#)

Network name (SSID)

Broadcast SSID ☒

VLAN ID (1 - 4094)

MAC authentication

Security method

Transfer key index

Key length ☐ 64 bits ☒ 128 bits

Key type ☐ ASCII ☒ Hex

Key 1 (26 characters)

Key 2

Key 3

Key 4

Authentication ☒ Open system ☐ Shared key

[Update](#) [Cancel](#)

Note

WEP cannot be used when the radio operating mode supports 802.11n or 802.11ac.

Transfer key index

This value indicates which of the four configured WEP keys the AP uses to encrypt the data it transmits.

Key length

The number of characters you specify for the key determines the level of encryption.

- For 64-bit encryption, specify 5 ASCII characters or 10 hexadecimal digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 hexadecimal digits.

Key type

Select the format used to specify the encryption key. The definition for the encryption key must be the same on the M330 and all wireless clients.

- **ASCII:** ASCII keys are much weaker than carefully chosen hexadecimal keys. You can include ASCII characters from 32 to 126, inclusive, in the key, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. However, note that not all wireless clients support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
- **Hex:** Your keys should only include the following hexadecimal characters: 0-9, a-f, A-F.

Key 1 to Key 4

Specify the key as ASCII or hexadecimal characters.

Authentication

The authentication algorithm defines the method used to determine whether a client is allowed to associate with an AP using WEP.

Choose one of the following options:

- **Open system:** This method allows any client to associate with the AP whether or not that client has the correct WEP key. It does not ensure, however, that an associated client can exchange traffic with the AP. A client must have the correct WEP key to be able to successfully access and decrypt data from an AP, and to transmit readable data to it.
- **Shared key:** This method requires the client to have the correct WEP key to associate with the AP. A client with an incorrect WEP key will not be able to associate with the AP.
- **Open system and shared key.** This is the default selection. When selected:
 - Wireless clients configured to use WEP in shared key mode must have a valid WEP key to associate with the AP.
 - Wireless clients configured to use WEP as an open system mode (shared key mode not enabled) can associate with the AP even if they do not have the correct WEP key.

Note

Open system authentication or shared key authentication can be used by the client to authenticate with the AP when the AP is configured for 802.11 open authentication. When the AP is configured for 802.11 shared key authentication, however, 802.11 shared key authentication must be used by the client to authenticate with the AP.

802.1X/Dynamic WEP

802.1X enables you to authenticate wireless clients via user accounts stored on a third-party RADIUS server. 802.1X is purely a protocol for user authentication. On the M330, it is paired with Dynamic WEP, which adds WEP encryption based on a set of dynamically generated keys.

Network name (SSID)	VLAN ID	MAC auth	Security	Delete
0 HP1_2.4G	1	Disabled	Disabled	

✖ = SSID Off ⓘ = SSID On ⓘ = SSID On and configured for broadcast

[Add New Wireless Community](#)

Network name (SSID)

Broadcast SSID ☒

VLAN ID (1 - 4094)

MAC authentication

Security method

Use global RADIUS server settings ☐

RADIUS IP address type ☒ IPv4 ☐ IPv6

RADIUS IP address

RADIUS IP address-1

RADIUS IP address-2

RADIUS IP address-3

RADIUS key (1 - 64 characters)

RADIUS key-1

RADIUS key-2

RADIUS key-3

Enable RADIUS accounting ☐

Broadcast key refresh rate (0 - 86400 seconds)

Session key refresh rate (30 - 86400 seconds, 0 disables)

[Update](#) [Cancel](#)

Note

Dynamic WEP cannot be used when the radio operating mode supports 802.11n or 802.11ac.

Use global RADIUS server

When selected, the wireless community will use the global RADIUS servers defined at the top of the Communities page. When not selected, you can configure each wireless community to use a different set of RADIUS servers.

RADIUS IP address type

You can toggle between the address types to configure IPv4 and IPv6 RADIUS server addresses. Note, however, that the AP contacts only the RADIUS server or servers of the address type selected in this field.

RADIUS IP address/RADIUS IPv6 address

Enter the IPv4 or IPv6 address for the primary RADIUS server for this wireless community.

If **IPv4** is selected as the **RADIUS IP address type**, enter the IP address of the RADIUS server that all wireless communities use by default, for example 192.168.10.23. If **IPv6** is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.

RADIUS IP or IPv6 address 1 to 3

Enter up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this wireless community. The field label is **RADIUS IP address** when **IPv4** is selected as the **RADIUS IP address type**, and **RADIUS IPv6 address** when **IPv6** is selected.

If authentication fails with the primary server, each configured backup server is tried in sequence.

RADIUS key

Enter the RADIUS key in the text box.

The RADIUS key is the shared secret key for the RADIUS server. You can use up to 63 alphanumeric and special characters. The key is case-sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as asterisk (*) characters to prevent others from seeing the RADIUS key as you type.

RADIUS key 1 to 3

Enter the RADIUS key associated with the configured backup RADIUS servers. The server at **RADIUS IP address-1** uses **RADIUS key-1**, **RADIUS IP address-2** uses **RADIUS key-2**, and so on.

Enable RADIUS accounting

Select this option to track and measure the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on.

If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.

Broadcast key refresh rate

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this wireless community (the default is 300).

The valid range is 0 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session key refresh rate

Enter the interval at which the AP will refresh session (unicast) keys for each client associated with the wireless community.

To enable session key refreshing, specify a value in the range of 30 to 86400 seconds. Specify a value of 0 to disable the refreshing of session keys.

WPA Personal

WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP mechanisms. It employs a preshared key (instead of using IEEE 802.1X and EAP, as is used in the WPA Enterprise mode). The preshared key (PSK) is used for an initial check of credentials only.

Network name (SSID)	VLAN ID	MAC auth	Security	Delete
0 HP1_2.4G	1	Disabled	WPA personal	

= SSID Off = SSID On = SSID On and configured for broadcast

[Add New Wireless Community](#)

Network name (SSID)

Broadcast SSID ☒

VLAN ID (1 - 4094)

MAC authentication

Security method

WPA versions ☐ WPA (TKIP) ☒ WPA2 (AES)

Protected management frames ☐ Disabled ☒ Supported ☐ Mandatory

Key (8 - 63 characters)

Confirm key

Broadcast key refresh rate (0 - 86400 seconds)

[Update](#) [Cancel](#)

WPA versions

Select one of the following options:

- **WPA (TKIP)**: WPA with TKIP encryption. This is the original version of the standard and is still supported by many legacy clients.
- **WPA2 (AES)**: WPA2 (802.11i) with AES encryption. This version is more secure than WPA (TKIP). If all your users have WPA2 client software, select this option for the maximum possible security.
- **WPA** and **WPA2**: When both are selected, both WPA and WPA2 are supported at the same time. Some legacy WPA clients may not work if this mode is selected. This mode is slightly less secure than using the WPA2 (AES/CCMP) mode.

Note

WPA2 (AES) must be selected when the radio mode supports 802.11n. If an 802.11n-only mode is selected, only WPA2 (AES) can be used.

Key

The M330 uses the preshared key (PSK) you specify to generate the WPA (TKIP) or WPA2 (AES) keys that are used to encrypt the wireless data stream. Specify a key that is from 8 to 63 alphanumeric characters in length. HP recommends that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The key cannot begin or end with spaces.

Broadcast key refresh rate

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this wireless community (the default is 300). The valid range is 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Protected management frames

Provides security for the otherwise unprotected and unencrypted 802.11 management frames. This configuration parameter is visible only when **WPA2 (AES)** security is enabled. The following three options can be configured:

- **Disabled:** Protected management frames are not used for clients.
- **Supported:** Capable clients can use protected management frames.
- **Mandatory:** Clients must be capable of using protected management frames to associate with the community.

By default **Supported** is selected. When selecting **Mandatory**, the **Supported** checkbox is also selected.

WPA Enterprise

WPA Enterprise with RADIUS is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes the CCMP (AES) and TKIP mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users.

Network name (SSID)	VLAN ID	MAC auth	Security	Delete
0 HP1_2.4G	1	Disabled	WPA personal	

= SSID Off = SSID On = SSID On and configured for broadcast

[Add New Wireless Community](#)

Network name (SSID)

HP1_2.4G

Broadcast SSID

☒

VLAN ID

1 (1 - 4094)

MAC authentication

Disabled

Security method

WPA enterprise

WPA versions

☐ WPA (TKIP) ☒ WPA2 (AES)

Protected management frames

☐ Disabled ☒ Supported ☐ Mandatory

Enable pre-authentication

☐

Use global RADIUS server settings

☒

RADIUS IP address type

☒ IPv4 ☐ IPv6

RADIUS IP address

RADIUS IP address-1

RADIUS IP address-2

RADIUS IP address-3

RADIUS key

(1 - 64 characters)

RADIUS key-1

RADIUS key-2

RADIUS key-3

Enable RADIUS accounting

☐

Broadcast key refresh rate

300 (0 - 86400 seconds)

Session key refresh rate

0 (30 - 86400 seconds, 0 disables)

Update

Cancel

WPA versions

Select the types of wireless clients you want to support:

- **WPA (TKIP):** If all wireless clients on the network support WPA but none support WPA2, then select WPA. WPA (TKIP) only is not allowed in 802.11n and 802.11ac modes.
- **WPA2 (AES):** If all wireless clients on the network support WPA2, we suggest using WPA2, which provides the best security per the IEEE 802.11i standard.

If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both **WPA (TKIP)** and **WPA2 (AES)**. This setting enables both WPA and WPA2 wireless clients to associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

Protected management frames

Provides security for the otherwise unprotected and unencrypted 802.11 management frames. This configuration parameter is visible only when **WPA2 (AES)** security is enabled. The following three options can be configured:

- **Disabled:** Protected management frames are not used for clients.
- **Supported:** Capable clients can use protected management frames.
- **Mandatory:** Clients must be capable of using protected management frames to associate with the community.

By default **Supported** is selected. When selecting **Mandatory**, the **Supported** checkbox is also selected.

Enable pre-authentication

If for WPA versions you select only **WPA2 (AES)** or both **WPA (TKIP)** and **WPA2 (AES)**, you can enable pre-authentication for WPA2 clients. Enable pre-authentication if you want WPA2 wireless clients to send pre-authentication packets. The pre-authentication information will be relayed from the AP the client is currently using to the target AP. Enabling this feature can help speed up authentication for roaming clients who connect to multiple APs.

Use global RADIUS server

When selected, the wireless community will use the global RADIUS servers defined at the top of the Communities page. When not selected, you can configure each the wireless community to use a different set of RADIUS servers.

RADIUS IP address type

You can toggle between the address types to configure IPv4 and IPv6 RADIUS server addresses. Note, however, that the AP contacts only the RADIUS server or servers of the address type selected in this field.

RADIUS IP address/RADIUS IPv6 address

Enter the IPv4 or IPv6 address for the primary RADIUS server for this wireless community.

If **IPv4** is selected as the **RADIUS IP address type**, enter the IP address of the RADIUS server that all wireless communities use by default, for example 192.168.10.23. If **IPv6** is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.

RADIUS IP or IPv6 address 1 to 3

Enter up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this wireless community. The field label is **RADIUS IP address** when **IPv4** is selected as the **RADIUS IP address type**, and **RADIUS IPv6 address** when **IPv6** is selected.

If authentication fails with the primary server, each configured backup server is tried in sequence.

RADIUS key

Enter the RADIUS key in the text box.

The RADIUS key is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case-sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.

RADIUS key 1 to 3

Enter the RADIUS key associated with the configured backup RADIUS servers. The server at **RADIUS IP address-1** uses **RADIUS key-1**, **RADIUS IP address-2** uses **RADIUS key-2**, and so on.

Enable RADIUS accounting

Select this option to track and measure the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on.

If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.

Broadcast key refresh rate

Enter the interval at which the broadcast (group) key is refreshed for clients associated with this wireless community (the default is 300).

The valid range is 0 to 86400 seconds. Specify a value of 0 to disable the refreshing of broadcast keys.

Session key refresh rate

Enter the interval at which the AP will refresh session (unicast) keys for each client associate with the wireless community.

To enable session key refreshing, specify a value in the range of 30 to 86400 seconds. Specify a value of 0 to disable session key refresh.

MAC authentication

You can control access to the wireless network based on the MAC address of a user's wireless device. You can either block access or allow access, depending on your requirements.

For each wireless community, you can select whether to disable MAC authentication, use a MAC authentication list stored locally on the M330, or use a list stored on a RADIUS server (see ["Wireless community configuration options" on page 32](#)).

Caution

MAC authentication is vulnerable to MAC address spoofing, where users in the network who are not granted access to the M330 gain access by changing their MAC addresses to an authorized user's address. For better security, administrators should consider using an additional authentication method (WPA Personal, WPA Enterprise, 802.1X/Dynamic WEP, or Static WEP). MAC authentication occurs after other authentication methods are applied.

RADIUS server-based MAC authentication

When RADIUS server-based MAC authentication is enabled on a wireless community, a wireless client MAC address is compared to the configured list stored on a RADIUS Server upon authentication. When a client MAC address is found in the configured list, the globally configured allow or deny action is applied to the client. When a client MAC address is not found in the list, the opposite allow or deny action is applied.

The following attributes must be configured on the RADIUS server:

- **User-Name (1):** Ethernet MAC address of the client.
- **User-Password (2):** A fixed password used to lookup a client MAC entry. The M330 uses the password "NOPASSWORD".

Local MAC authentication

Select **Wireless > MAC authentication** to configure the local MAC authentication list. You can use this page to configure a local list, which applies to every wireless community on which local MAC authentication is enabled.

MAC Authentication ?

Local MAC authentication configuration

Filter

☐ Allow only stations in list

☒ Block all stations in list

Local MAC authentication client list

MAC address : : : : : Add

Client list

Remove

Save Cancel

Filter

Select one of the following options:

- **Allow only stations in list:** Only users whose MAC addresses appear in the MAC address list can connect to the wireless network created by this community.
- **Block all stations in list:** Users whose MAC address appear in the MAC address list are blocked from accessing the wireless network created by this community.

Stations list

Up to 512 MAC addresses are supported. To remove an address, select it in the list and select **Remove**.

MAC address

To add a MAC address, specify six pairs of hexadecimal digits separated by colons (for example, 00:00:00:0a:0f:01), and then select **Add**. The added address appears in the Stations list.

5 Wireless configuration

Wireless coverage

As a starting point for planning your network, you can assume that when operating at high power, the M330 radio provides a wireless networking area (also called a wireless cell) of up to 92 meters (300 feet) in diameter. Before creating a permanent installation, you should always perform a site survey to determine the optimal settings and location for the M330.

The following sections provide information on wireless coverage. A tool that can help simplify planning a secure wireless network is the HP RF Planner (available separately). For more information, see the HP Networking website at <http://www.hp.com/go/networking> and search for RF Planner or contact your HP Partner.

Factors limiting wireless coverage

Wireless coverage is affected by the factors discussed in this section.

Interference

Interference is caused by other APs or devices that operate in the same frequency band as the M330 and can substantially affect throughput. Several tools are available to diagnose interference problems as they occur.

- Select **Wireless > Rogue AP Detection** to view detailed information about all wireless APs operating in the immediate area so that you can effectively set the operating frequencies. This feature also makes it easy for you to find rogue APs. See “[Detecting rogue APs](#)” on page 58.
- Select **Status > Wireless** to view detailed information about packets sent and received, transmission errors, and other low-level events.

Caution

APs that operate in the 2.4 GHz band may experience interference from devices including 2.4 GHz cordless phones and microwave ovens. A smaller but growing number of devices are potential sources of interference in the 5 GHz band.

Physical characteristics of the location

To maximize coverage of an M330, install it in an open area with as few obstructions as possible. Try to choose a location that is central to the area being served.

Radio waves cannot penetrate metal—they are reflected instead. The M330 can transmit through wood or plaster walls and closed windows (although window glazing or thickness may impair penetration). However, the steel reinforcing found in concrete walls and floors may block transmissions or reduce signal quality by creating reflections. This can make it difficult or impossible for a single M330 to serve users on different floors in a concrete building. Such installations require a separate M330 on each floor.

Configuring overlapping wireless APs

When the radio is operating in the 2.4 GHz band and two or more APs are within transmission range of each other, they may use overlapping channels. This may be under your control (for example, when you use several APs to cover a large location) or out of your control (for example, when your neighbors set up their own wireless networks). In either case, the problems you face are similar.

Note

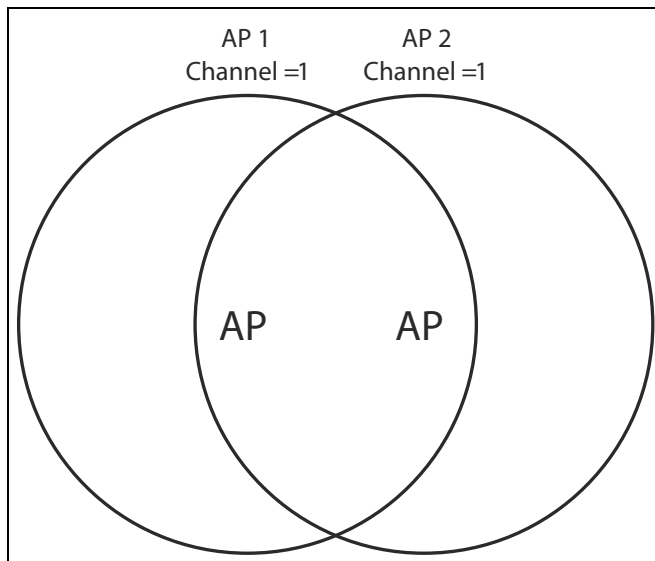
Overlapping channels do not occur when the radio is operating in the 5 GHz band. All 5 GHz channels are non-overlapping.

Performance degradation and channel separation

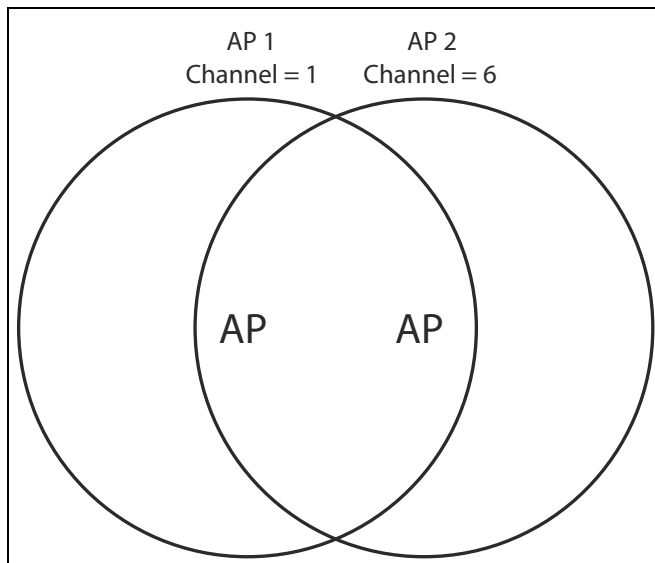
When two wireless APs operating on the same frequency overlap, throughput can be reduced in both APs. Reduced throughput occurs because a wireless user that is attempting to transmit data defers (delays) transmission if another station is transmitting. In a network with many users and much traffic, these delayed transmissions can severely affect performance because wireless users may defer several times before the channel becomes available. If a wireless user is forced to delay transmission too many times, data can be lost.

Delays and lost transmissions can severely reduce throughput on a network. To view this information about your network, select **Status > Wireless**.

The following example shows two overlapping wireless APs operating on the same frequency. Since the APs are within range of each other, the number of deferred transmissions can be large.



The solution to this problem is to set the two networks to different channels with as great a separation as possible in their operating frequencies. This reduces crosstalk and enables wireless clients connected to each M330 to transmit at the same time.



Selecting channels

For optimal performance when operating in the 2.4 GHz band, select an operating frequency that is different by at least 25 MHz from the frequency used by neighboring APs.

Two channels with the minimum 25 MHz frequency separation always perform worse than two channels that use maximum separation. It is always best to use the greatest separation possible between overlapping networks.

With the proliferation of wireless networks, it is very possible that the areas of coverage of APs outside your control overlap your intended area of coverage. To choose the best operating frequency, select **Wireless > Rogue AP Detection** to generate a list of all APs that operate near you and their operating frequencies.

The number of non-overlapping channels available to you varies by geographical location, which affects how you set up your network when multiple APs are present.

Sample channel selections

For example, when operating in 802.11b mode, the M330 supports the following 14 channels in the 2.4 GHz band:

Channel	Frequency	Channel	Frequency
1	2412	8	2447
2	2417	9	2452
3	2422	10	2457
4	2427	11	2462
5	2432	12	2467
6	2437	13	2472
7	2442	14	2477

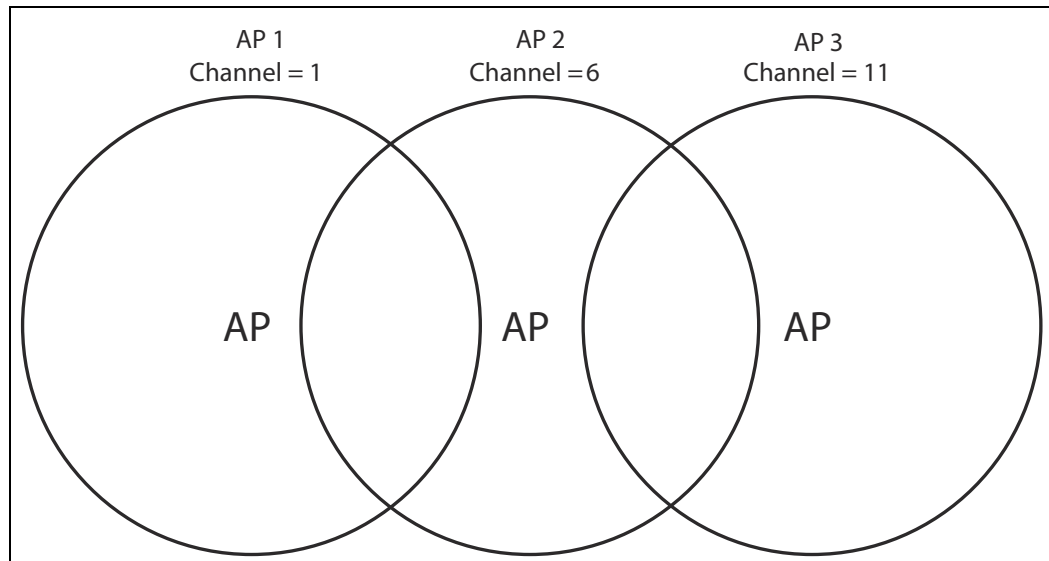
However, the number of channels available for use in a particular country are determined by regional regulations. The following table shows the number of channels that are available in North America and Europe:

Region	Available channels
North America	1 to 11
Europe	1 to 13

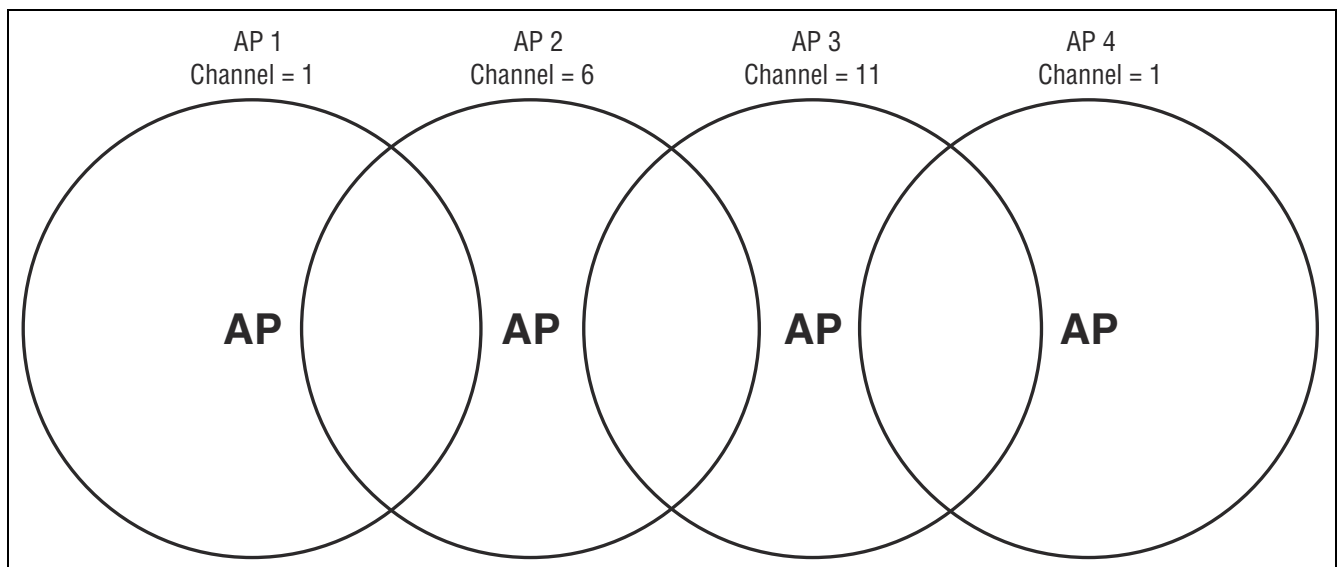
Since the minimum recommended separation between overlapping channels is 25 MHz (in other words, they must be at least five channels apart) the recommended maximum number of overlapping APs you can have in most regions is three. The following table gives examples relevant to North America and Europe for channels in the 2.4 GHz band:

North America	Europe
<ul style="list-style-type: none">• AP 1 on channel 1• AP 2 on channel 6• AP 3 on channel 11	<ul style="list-style-type: none">• AP 1 on channel 1• AP 2 on channel 7• AP 3 on channel 13

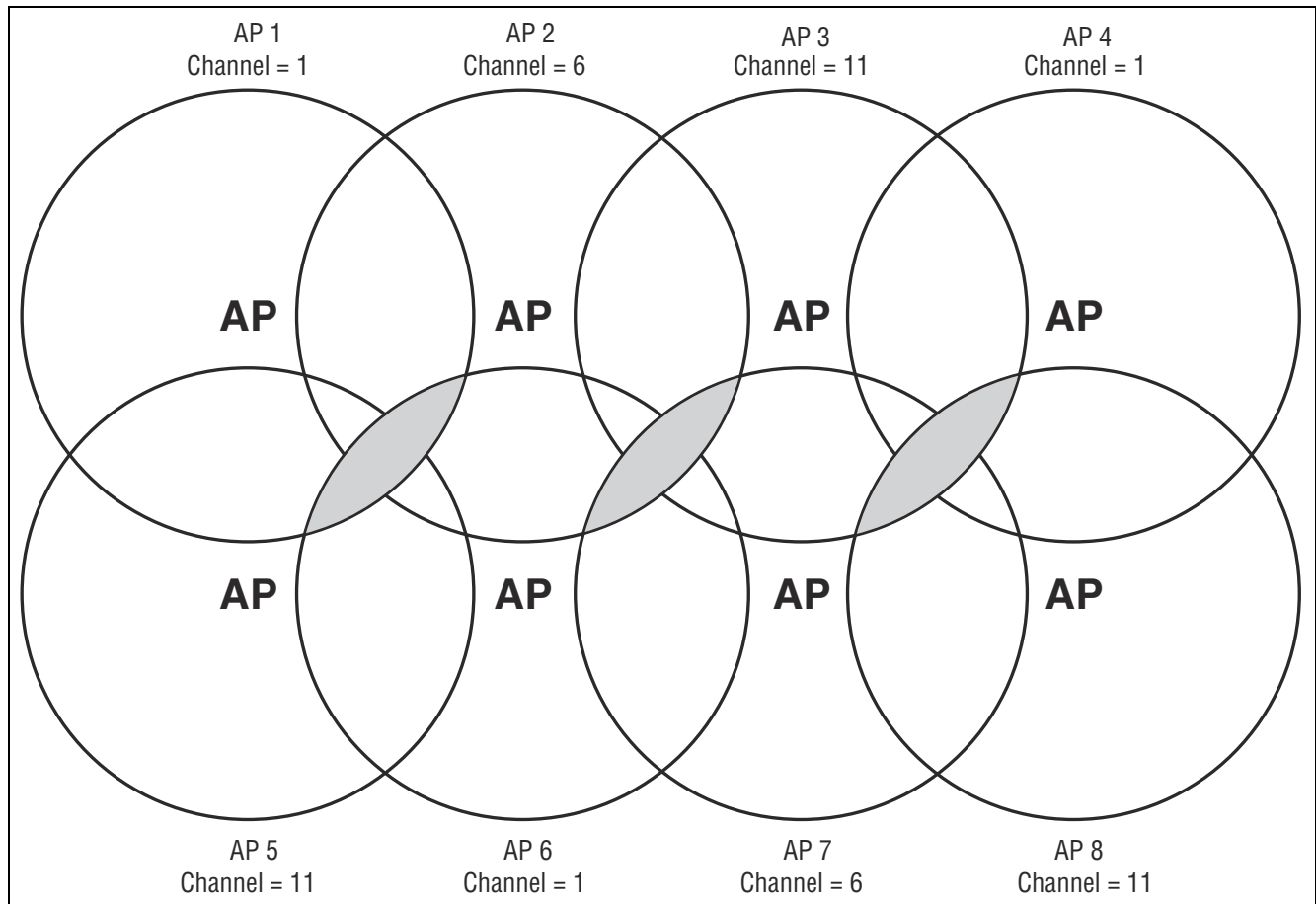
In North America, you can reduce transmission delays by using different operating frequencies, as shown in the following figure:



Alternatively, you can stagger APs to reduce overlap and increase channel separation, as shown in the following figure:



This strategy can be expanded to cover an even larger area using three channels, as shown in the following figure:



802.11ac and 802.11n best practices

This section provides recommendations on how to best use 802.11ac and 802.11n wireless technologies, especially when legacy (a/b/g) clients must also be supported.

Supporting legacy wireless clients

The 802.11n standard is very similar to the 802.11g standard, in that both provide mechanisms to support older wireless standards. In the case of 802.11g, protection mechanisms were created to allow 802.11b and 802.11g wireless devices to co-exist on the same frequencies despite using different signal modulation schemes. Since older 802.11b-only clients cannot detect the newer 802.11g modulation scheme, 802.11g clients must “protect” their transmissions by first sending a signal that alerts 802.11b clients to not attempt to transmit for a specified period of time.

If protection is not used, 802.11b clients may transmit while an 802.11g frame is already being sent. This leads to a collision and both devices need to re-transmit. If there are enough devices in the network, the collision rate will grow exponentially and prevent any useful throughput from the wireless network.

802.11n clients face the same problem as described for 802.11g clients. Legacy a/b/g clients cannot detect the High Throughput (HT) rates that 802.11n uses. To avoid causing excessive collisions, 802.11n clients must use the same protection mechanisms when a legacy client is present. Even the most efficient protection mechanism (CTS-to-self) causes a substantial decline in throughput. Performance can decline by as much as 50 percent. The 802.11n clients can achieve maximum data rates only when the legacy clients are not present.

The 802.11ac standard is an extension of the 802.11n standard that operates only in the 5 GHz band. As well as operating in the less-crowded 5 GHz band, the 802.11ac standard was designed to be seamlessly compatible with legacy 802.11a/n devices. The 802.11ac standard automatically falls back to 802.11a/n operation when 802.11a/n clients are detected.

Compatibility modes

See [“Basic settings” on page 51](#) for a list of supported modes.

Modes that support multiple 802.11 standards are referred to as compatibility modes. For the 2.4 GHz radio, IEEE 802.11b/g/n is the default mode, and for the 5 GHz radio, 802.11a/n/ac is the default mode.

For compatibility modes that support 802.11n clients, the M330 advertises protection in its beacon frames when legacy clients are associated or operating on the same channel. This alerts the associated 802.11n clients to use protection when transmitting. The M330 also uses protection when necessary while sending HT data.

Compatibility for 802.11ac in the 5 GHz band operates in a similar way as 802.11n in the 2.4 GHz band, with the M330 using protection when sending VHT data.

Compatibility modes should be used when legacy clients are present in the network. HP recommends IEEE 802.11a/n/ac or IEEE 802.11b/g/n as the typical operating mode. Both modes allow for all wireless clients to connect and they use protection to avoid causing interference.

IEEE 802.11n (2.4 GHz)

HP refers to this mode as Pure-n. When the M330 2.4 GHz radio is in this mode, it will not allow non-802.11n clients to associate. Legacy clients can see the M330, and may attempt to associate, but they will be rejected. The M330 makes this determination based on information on supported capabilities that the client presents during its association request. If the client does not indicate support for 802.11n capabilities, it is not allowed to associate.

In this mode, the M330 will not use protection when sending HT frames to associated clients. If legacy APs or clients are using the same channel, this may lead to collisions. In the 2.4 GHz band, this mode may cause serious performance deterioration for everyone on the channel (both the 802.11b/g and 802.11n clients).

The M330 still signals associated clients to use protection when they send data. The M330 does this via a field in the beacons that it sends. So clients sending data to the M330 will use protection, but data sent from the M330 will not be protected.

Note

Some people may refer to this mode as Greenfield, which is not correct. Greenfield is an 802.11n-specific preamble. The M330 does not support this preamble and therefore does not support Greenfield mode.

The Pure-n mode can be used when there is no legacy wireless traffic present in or around the premises on the channels that will be used. All client devices must support 802.11n.

Channel width

When operating in an 802.11n mode, the M330 enables you to use the standard channel width of 20 MHz or a double width of 40 MHz. A width of 40 MHz is achieved by using two adjacent channels to send data simultaneously. The advantage of using a 40 MHz wide channel is that the available bandwidth is doubled, leading to much higher throughput for clients operating in that mode. A disadvantage is that fewer channels are available for use by all clients.

When the channel width is set to **20 MHz**, channel usage is the same as in legacy mode.

When **40 MHz** is selected, the M330 radio uses a 40 MHz channel width. However, both 20 MHz and 40 MHz clients can associate. The channel selected on the **Radio** page is the primary channel and the secondary (or extension) channel is located adjacent to it. The secondary channel is either above or below depending on which channel was selected as the primary. In 5 GHz IEEE 802.11n mode, the channels are paired: for example, channels 36 and 40 are always used together, 44 and 48 are always used together, etc.

Note

If the **Country** setting identifies a regulatory domain that does not support the 40 MHz channel bandwidth, this setting does not apply.

The 802.11ac standard in the 5 GHz band supports channel widths of 20 MHz, 40 MHz, and 80 MHz. The **80 MHz** option bonds two 40 MHz channels to form one high-throughput channel. Note that in the 5 GHz band, a channel bandwidth of 80 MHz can reduce the number of available channels to four.

Radio configuration

To define configuration settings for the M330 radio, select **Wireless > Radio**. The radio settings page displays.

Radio

Country

Country US - United States

Basic settings

Radio 1

Status ☒ On ☐ Off

Mode IEEE 802.11b/g/n

Channel Auto

Channel bandwidth 20 MHz

Primary channel Lower

Current channel 1 (2412 MHz)

Station isolation ☐

Advanced settings

Save Cancel

This page enables you to configure the country in which the M330 operates, basic radio settings such as the radio mode and channel, and advanced radio features.

Country

The country of operation, also known as the regulatory domain, determines the availability of certain wireless settings on the M330.

Once the country has been set, the M330 automatically limits the available wireless channels and channel width, and adjusts the radio power level in accordance with the regulations of the selected country.

Caution

Incorrectly selecting the country may result in illegal operation and may cause harmful interference to other systems. Ensure that the M330 is operating in accordance with channel, power, indoor/outdoor restrictions, and license requirements for the intended country. If you fail to heed this caution, you may be held liable for violating the local regulatory compliance.

Basic settings

Radio

Selects the radio interface. Select **1** for the 2.4 GHz radio or **2** for the 5 GHz radio.

Status

By default, both radios are set to **On**. If you set the selected radio to **Off**, all associated wireless clients are disassociated and no wireless clients can connect.

Mode

Select the mode that best supports the wireless clients at your location.

Supported wireless modes are determined by the regulatory domain (country). Available options may include one or more of the following:

- **IEEE 802.11b/g:** (Compatibility mode.) Up to 11 Mbps for 802.11b and 54 Mbps for 802.11g in the 2.4 GHz frequency band. Use this setting only when support for 802.11b is necessary and support for 802.11n is not desired.
- **IEEE 802.11b/g/n:** (Compatibility mode.) Up to 11 Mbps for 802.11b, 54 Mbps for 802.11g, and 450 Mbps for 802.11n in the 2.4 GHz frequency band. Use this setting when support for 802.11b and 802.11g is necessary.
- **2.4 GHz IEEE 802.11n:** (Pure 802.11n) Up to 450 Mbps in the 2.4 GHz frequency band.
- **IEEE 802.11a:** Up to 54 Mbps for 802.11a in the 5 GHz frequency band.
- **IEEE 802.11a/n/ac:** (Compatibility mode.) Up to 1.3 Gbps for 802.11ac, 450 Mbps for 802.11n, and 54 Mbps for 802.11a in the 5 GHz frequency band.
- **IEEE 802.11n/ac:** (Compatibility mode.) Up to 450 Mbps for 802.11n and 1.3 Gbps for 802.11ac in the 5 GHz frequency band.

Note

In **2.4 GHz IEEE 802.11n** mode, the M330 does not permit non-802.11n clients to associate. Also in this mode, the M330 does not use protection mechanisms (RTS/CTS or CTS-to-self) to enable legacy APs to operate on the same frequency. This can potentially cause problems with legacy (802.11a/b/g) APs operating on the same channel, but provides the best throughput for the M330 and its 802.11n clients.

In **IEEE 802.11a/n/ac**, and **IEEE 802.11b/g/n** modes, the M330 permits both 802.11n and legacy clients (802.11a/b/g) to associate. The M330 uses protection mechanisms (RTS/CTS or CTS-to-self) when sending 802.11n data to prevent disruption to legacy (802.11a/b/g) clients associated on the same channel. For more information, refer to [“802.11ac and 802.11n best practices” on page 48](#).

Channel

Select the channel for wireless services. The range of available channels is determined by the mode of the radio interface and the country code setting.

- Automatic channel selection. If you select **Auto** for the channel setting, a channel is automatically selected as follows:
 - If the AP is operating in a 2.4 GHz radio mode, the AP scans all valid channels in the current radio band and selects the channel with the least number of APs found.
 - If the AP is operating in a 5 GHz radio mode and is deployed in a country where Dynamic Frequency Selection (DFS) is supported, then the AP randomly selects a channel from the list of valid channels for the country and radio mode. If DFS is not supported, then the AP scans all valid channels for the current radio band and selects the channel with the least number of APs found.

The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).

- Manual channel selection

If setting the channel manually, for optimal performance when operating in 2.4 GHz modes, select a channel that is different by at least five channel numbers (25 MHz) from the channels used on wireless APs that have overlapping coverage areas. For example, if another AP is operating on channel 1, set the M330 to channel 6 or higher. Select **Wireless > Rogue AP Detection** to view a list of APs currently operating in your area.

When operating in 802.11a or 5 GHz 802.11n modes, all channels are non-overlapping, so you can configure APs to operate on adjacent channels.

Note

Channel selection for APs in a cluster: When automatic channel assignment is enabled on the **Cluster > Channel planning** page, the channel policy for the radio is automatically set to static mode, and the **Auto** option is not available for the Channel setting. This configuration allows the automatic channel feature to set the channels for the radios in the cluster.

Channel bandwidth

(Only applicable when **Wireless mode** includes some type of 802.11n or 802.11ac support.)

Select the **Channel width** that will be used for 802.11n or 802.11ac users.

- **20 MHz:** Sets channel width to 20 MHz.
- **40 MHz:** Under most conditions, this can double throughput by bonding adjacent channels to form a 40 MHz channel. This option reduces the number of unoccupied channels available to neighboring APs.
- **80 MHz:** For 802.11ac channels, a bandwidth of 80 MHz can be set for increased throughput. This option bonds two 40 MHz channels to form an 80 MHz channel.

Note

Although some 802.11n clients only support 20 MHz channels, they can still associate with a M330 configured for **40 MHz**.

Primary channel (802.11n modes only)

This setting can be changed only when the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary channel is used for 802.11n clients that support only a 20 MHz channel bandwidth and for legacy clients.

Select one of the following options:

- **Upper:** The Primary Channel is the upper 20-MHz channel in the 40-MHz band.
- **Lower:** The Primary Channel is the lower 20-MHz channel in the 40-MHz band.

Current channel

This field displays the currently assigned channel.

Station isolation

When enabled, the M330 prevents communication between wireless clients associated with the same wireless community. Clients can still communicate with the wired network, across a WDS link, and with other wireless clients associated with a different wireless community. This selection is applied to all wireless communities on the AP.

Advanced radio settings

When you select **+** next to **Advanced settings**, the following settings display:

Advanced settings

DFS Support

On

Multidomain regulatory mode

Enable

Short guard interval supported

Yes

STBC mode

On

Protection

Auto

Beacon Interval

100

(20 - 2000 msec)

DTIM period

2

(1 - 255 beacons)

Fragmentation threshold

2346

(256 - 2346 bytes, even numbers)

RTS threshold

2347

(0 - 2347 bytes)

Transmit power

100

(1 - 100 percent)

Fixed multicast rate

Auto

Mbps

☐ Broadcast/Multicast rate limiting

Rate limit

50

(1 - 50 packets per second)

Rate limit burst

75

(1 - 75 packets per second)

Save

Cancel

DFS support

(5 GHz, radio 2 only) Dynamic Frequency Selection (DFS) is a mechanism that enables wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5 GHz band. The DFS requirements vary depending on the configured regulatory domain.

Multidomain regulatory mode

This mode causes the AP to broadcast, as a part of its beacons and probe responses, the country in which it is configured for operation. This allows wireless clients to operate in any country without reconfiguration.

Disabling this feature prevents the country code setting from being broadcast in the beacons. However, this applies only to radios configured to operate in the 802.11g band (2.4 GHz). For radios operating in the 802.11a band (5 GHz), the AP software configures support for the IEEE standard 802.11h. When 802.11h is supported, the country code information is broadcast in the beacons.

Short guard interval supported

This setting is available only if the selected radio mode includes 802.11n.

The guard interval is the dead time, in nanoseconds, between symbols (or characters) transmitted by the AP. The guard interval helps distinguish where one symbol transmission stops and another starts, thereby reducing inter-symbol interference (ISI). The 802.11n mode allows for a reduction in this guard interval from the 802.11a and 802.11g definition of 800 nanoseconds to 400 nanoseconds. Enabling the short guard interval (SGI) is recommended, as it can yield a 10% improvement in data throughput.

Note

If SGI is enabled on the M330 but a wireless client does not support SGI, the client will be able to communicate with M330 at a data rate that is about 10% slower than SGI-enabled clients.

Select one of the following options:

- **Yes** (default): AP transmits data using a 400 ns guard interval when communicating with clients that also support the short guard interval.

- **No:** The AP transmits data using an 800 ns guard interval.

STBC mode

This setting is available only if the selected radio mode includes 802.11n.

Space Time Block Coding (STBC) is an 802.11n technique that improves the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams. Enabling STBC results in a lower but more stable throughput.

Select one of the following options:

- **On:** AP transmits the same data stream on multiple antennas at the same time.
- **Off:** The AP does not transmit the same data on multiple antennas.

Protection

The protection feature provides rules to guarantee that 802.11n and 802.11g transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (**Auto**). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP.

You can disable these protection mechanisms (**Off**). When protection is off, however, legacy clients or APs within range can be affected by 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions.

Note

This setting does not affect the ability of the client to associate with the AP.

Beacon interval

Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (10 per second).

Enter a value from 20 to 2000 milliseconds.

DTIM period

Specify a DTIM period from 1 to 255 beacons.

The Delivery Traffic Information Map (DTIM) message is an element included in some beacon frames. It indicates which wireless clients, currently sleeping in low-power mode, have data buffered on the AP awaiting pickup.

The DTIM period you specify indicates how often the clients served by this AP should check for buffered data still on the AP awaiting pickup.

The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.

Fragmentation threshold

Specify a number from 256 to 2,346 to set the frame size threshold in bytes.

The fragmentation threshold is a way of limiting the size of frames transmitted over the network. If a frame exceeds the fragmentation threshold you set, the fragmentation function is activated and the frame is sent as multiple 802.11 frames.

If the frame being transmitted is equal to or less than the threshold, fragmentation is not used.

Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.

Fragmentation involves more overhead because it requires the extra work of dividing up and reassembling frames and it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured.

Sending smaller frames (by using lower fragmentation threshold) might help with some interference problems; for example, with microwave ovens.

By default, fragmentation is off. HP recommends not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

RTS threshold

Specify a Request to Send (RTS) threshold value from 0 to 2347.

The RTS threshold indicates the number of octets in an MPDU below which an RTS/CTS handshake is not performed.

Changing the RTS threshold can help control traffic flow through the AP, especially one with many clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce packet throughput on the AP. On the other hand, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network or on a network experiencing electromagnetic interference.

Transmit power

Enter a percentage value for the transmit power level for this AP.

The default value, which is 100%, can be more cost-efficient than a lower percentage, since it gives the AP a maximum broadcast range and reduces the number of APs needed to cover an area.

To increase the capacity of the network, place APs closer together and reduce the value of the transmit power. This helps reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.

Fixed multicast rate

This value sets a fixed transmission rate in Mbps for broadcast and multicast packets. This setting can be useful in an environment where wireless multicast video streaming occurs, provided the wireless clients are capable of handling the configured rate.

Select **Auto** to have the M330 choose the best rate automatically. The range of valid values is determined by the configured radio mode. The default value is **Auto**.

Bcast/Mcast rate limiting

Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. Note, however, that the performance of client applications that rely on multicast or broadcast traffic may be affected.

The rate limit applies only to traffic flowing in the downstream direction, from the AP to wireless clients.

By default, this option is disabled. When you enable it, the following fields are editable:

Rate limit

Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1 but less than 50 packets per second. Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination.

The default and maximum rate limit setting is 50 packets per second.

Rate limit burst

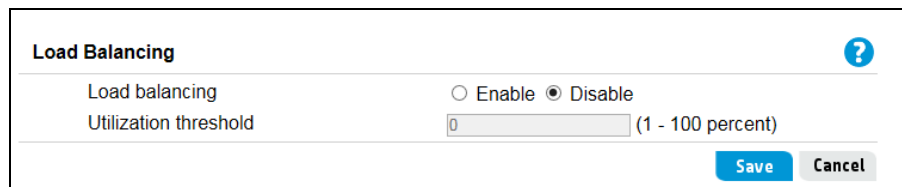
The rate limit burst sets a threshold rate for traffic bursts, above which all traffic is considered to exceed the rate limit. This burst limit allows intermittent bursts of traffic that are above the set **Rate limit**, but below the **Rate limit burst**.

The default and maximum rate limit burst setting is 75 packets per second.

Load balancing

You can set network utilization thresholds on the AP to maintain the speed and performance of the wireless network as clients associate and disassociate with the AP. The load balancing settings apply to both radios.

To configure load balancing settings for the M330 radios, select **Wireless > Load Balancing**. The **Load Balancing** page displays.



Load Balancing	
Load balancing	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Utilization threshold	<input type="text" value="0"/> (1 - 100 percent)
<div>Save Cancel</div>	

Load balancing

Enables or disables load balancing. To enable load balancing on this AP, click Enable. To disable load balancing on this AP, click Disable.

Utilization threshold

Provides the percentage of network bandwidth utilization allowed on the radio before the AP stops accepting new client associations. The default is 0, which means that all new associations are allowed regardless of the utilization rate.

Note

After configuring load balancing settings, click **Save**. Changing settings can cause the AP to stop and restart, temporarily losing connectivity for wireless clients. HP recommends changing AP settings only at times when users are not inconvenienced.

Detecting rogue APs

You can use the **Rogue AP Detection** feature to scan for other APs operating nearby. Initially, new APs on the network are identified as rogue APs. If you are aware of an AP detected as a rogue AP, and know that its existence on your network is legitimate, you can identify it as a *known AP* so that it will not continue to be detected as a rogue AP. This is useful for monitoring the installation of wireless APs in your company’s work areas to ensure that new APs (which could be a security risk if improperly configured) are not deployed without your knowledge.

This feature can also be used to determine the operating frequencies and signal strengths of nearby APs for site planning purposes.

Enabling scanning

Scanning for rogue APs is enabled by default. To disable it, select **Wireless > Rogue AP Detection**, select **Disable** next to **AP Detection for radio 1/2**, and then select **Save**.

Rogue AP Detection?

Rogue AP configuration

AP detection for radio 1

☒ Enable ☐ Disable

AP detection for radio 2

☒ Enable ☐ Disable

Save

When enabled, the AP initiates a scan on a single channel. Every 60 seconds, the AP scans the next sequential channel. The scan duration is 10 ms per channel.

Note

- Scanning is temporarily disabled when a trace is active (see the **Tool > Network Trace** page).
- Although the impact of scanning on AP performance is expected to be minimal, to obtain the best possible wireless performance (as needed for voice applications, for example), disable scanning.

Detected and known AP lists

When the M330 discovers an AP during a scan, it compares the MAC address of the AP against the **Known AP list** (a list that you create or import using the capabilities on this page). If the scanned AP does not appear in the list of known APs, it is displayed in the **Detected rogue AP list**.

Detected rogue AP list


MAC address	Radio	Beacon Int.	SSID	Privacy/WPA	Band/Channel	Signal	Action
18:59:36:f3:d6:6d	wlan0	100	Redrice	On / On	2.4 / 6	<div></div> -93	Grant

Refresh

The following information displays for each detected rogue AP:

Field	Description
MAC address	The MAC address of the neighboring AP detected during a scan.
Radio	Displays the 2.4 GHz (wlan0) or 5 GHz band (wlan1) on which the AP is detected.
Beacon Int.	The Beacon interval being used by this AP. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (10 per second).
SSID	The Service Set Identifier (SSID) for the AP. The SSID uniquely identifies a wireless LAN and is also referred to as the Network Name. It can be up to 32 alphanumeric characters.
Privacy	Whether there is any security on the neighboring device. <ul style="list-style-type: none"> • Off indicates that the Security mode on the neighboring device is set to None (no security). • On indicates that the neighboring device has some security in place.
WPA	Whether WPA security is on or off for this AP.
Band	The 802.11 band used on this AP, as follows: <ul style="list-style-type: none"> • 2.4 indicates 802.11b, 802.11g, or 802.11n mode (or a combination of the modes). • 5 indicates 802.11a, 802.11n, or 802.11ac mode (or all modes).
Channel	The channel on which the AP is currently broadcasting. The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The channel is set in the Radio settings. (See “Radio configuration” on page 51.)
Rate	The rate (in megabits per second) at which this AP is currently transmitting.
Signal	The detected strength of the radio signal from this AP in decibels (dB).

For any AP that is known to you, you can select **Grant** to move the AP to the **Known AP list**.

Known AP list							
MAC address	Radio	Type	SSID	Privacy	Band	Channel	Action
18:59:36:f3:d6:6d	wlan0	AP	Redrice	On	2.4	6	

You can select **Delete** to remove an AP from the **Known AP list**.

Note

The **Detected rogue AP list** and **Known AP list** provide information only. The M330 does not have control over the APs on these lists and cannot apply any security policies to them.

Working with saved AP lists

You can save the **Known AP list** and import a saved list to the M330. A saved list can show APs that you previously identified as known APs but that may not be showing in the current **Detected rogue AP list** (because they are not currently operational, for example).

To create a list, under **Save AP list**, select **Save** and then save the file to your PC or network.

Save AP list
Save known AP list to a file

Save

By default, the filename is Rogue2.cfg. You can use a text editor or web browser to open the file and view its contents.

In the **Import known AP list** section, you can import a list that was previously saved from this AP or from another M330.

Import known AP list
Replace or merge to known AP list
Filename

☒ Replace ☐ Merge

Browse...

Import

Select one of the following options:

- **Replace:** The imported list will replace the **Known APs list**.
- **Merge:** APs from the imported list are added to the existing **Known APs list**.

Browse to select the file to import, and select **Import**. The new list displays in the **Known AP list**.

Viewing wireless information

The M330 provides several pages where you can view information related to wireless operation.

Viewing all connected wireless clients

Select **Wireless > Client connections**.

The following information is displayed for each client currently connected to the M330:

Field	Description
Network	The wireless community the client is associated with. For example, an entry of wlan0vap2 means the client is associated with Radio 1, wireless community 2. An entry of wlan0 means the client is associated with community 0 on Radio 1. An entry of wlan1 means the client is associated with community 0 on Radio 2.
Station	The MAC address of the associated wireless client.

Field	Description
Status (Auth and Assoc)	<p>The underlying IEEE 802.11 authentication and association status, which is present no matter which type of security the client uses to connect to the AP. This status does not show IEEE 802.1X authentication or association status.</p> <p>Keep the following points in mind with regard to this field:</p> <ul style="list-style-type: none"> • If the Security method is None or Static WEP, the authentication and association status of clients showing on the Client Connections page are in line with what is expected; that is, if a client shows as authenticated to the AP, it is able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.) • If the Security method is IEEE 802.1X, WPA Personal, or WPA Enterprise, it is possible for a client to show on this tab as authenticated (via the IEEE 802.11 security) but actually not be authenticated to the AP via the second layer of security.
From station	The number of packets and bytes received from the wireless client and the number of packets and bytes that were dropped after being received.
To station	The number of packets and bytes transmitted from the AP to the wireless client and the number of packets and bytes that were dropped upon transmission.

Viewing wireless statistics for the radio

Select **Status** > **Wireless** to display the *Wireless status* page.

Wireless	
Wireless status	
Radio	1 ▾
WLAN packets received	0
WLAN bytes received	0
WLAN packets transmitted	4555
WLAN bytes transmitted	898106
WLAN packets receive dropped	0
WLAN bytes receive dropped	0
WLAN packets transmit dropped	0
WLAN bytes transmit dropped	0
Fragments received	0
Fragments transmitted	0
Multicast frames received	0
Multicast frames transmitted	4555
Duplicate frame count	0
Failed transmit count	0
Transmit retry count	0
Multiple retry count	0
RTS success count	0
RTS failure count	0
ACK failure count	0
FCS error count	1056
Transmitted frame count	4555
WEP undecryptable count	0
Refresh	

This page displays the following information:

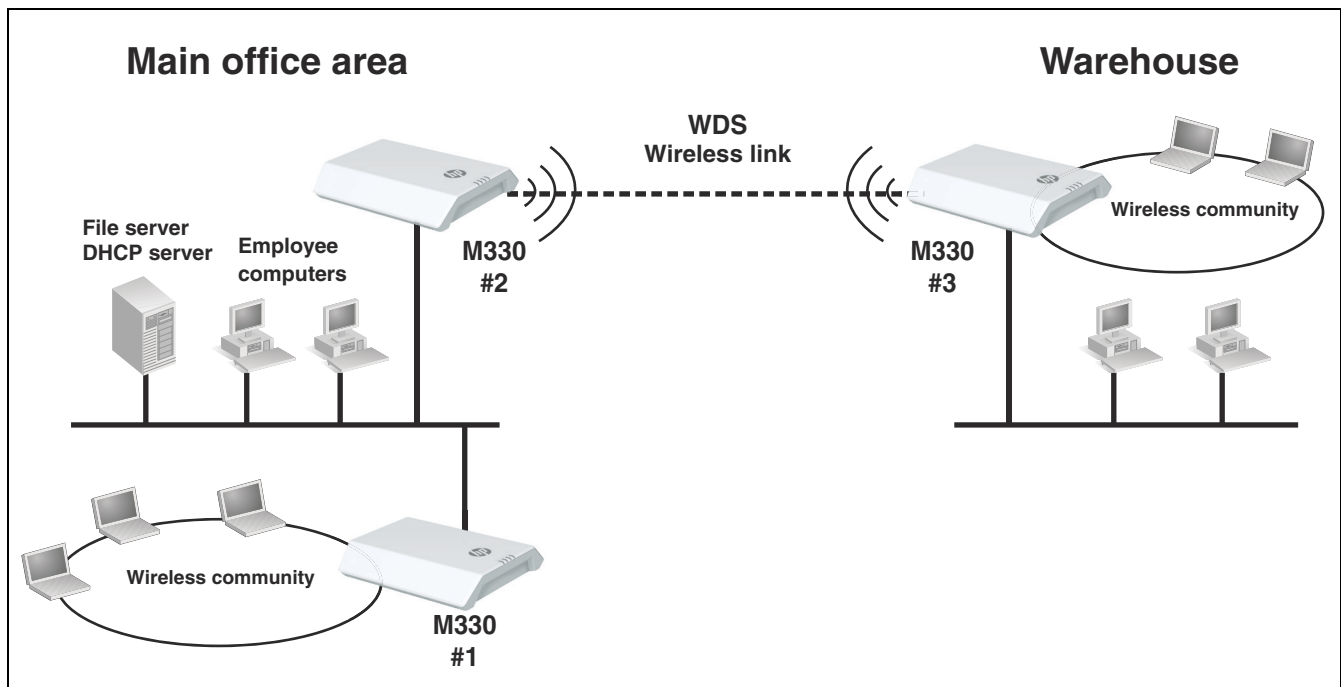
Field	Description
WLAN packets received	Total packets received by the AP.
WLAN bytes received	Total bytes received by the AP.
WLAN packets transmitted	Total packets transmitted by the AP.
WLAN bytes transmitted	Total bytes transmitted by the AP.
WLAN packets receive dropped	Number of packets received by the AP that were dropped.
WLAN bytes receive dropped	Number of bytes received by the AP that were dropped.
WLAN packets transmit dropped	Number of packets transmitted by the AP that were dropped.

Field	Description
WLAN bytes transmit dropped	Number of bytes transmitted by the AP that were dropped.
Fragments received	Count of successfully received MPDU frames of type data or management.
Fragments transmitted	Number of transmitted MPDU with an individual address or an MPDU with a multicast address of type data or management.
Multicast frames received	Count of MSDU frames received with the multicast bit set in the destination MAC address.
Multicast frames transmitted	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
Duplicate frame count	Number of times a frame is received and the Sequence Control field indicates it is a duplicate.
Failed transmit count	Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
Transmit retry count	Number of times an MSDU is successfully transmitted after one or more retries.
Multiple retry count	Number of times an MSDU is successfully transmitted after more than one retry.
RTS success count	Count of CTS frames received in response to an RTS frame.
RTS failure count	Count of CTS frames not received in response to an RTS frame.
ACK failure count	Count of ACK frames not received when expected.
FCS error count	Count of FCS errors detected in a received MPDU frame.
Transmitted frame count	Count of each successfully transmitted MSDU.
WEP undecryptable count	Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

6 Creating WDS links

Key concepts

The Wireless Distribution System (WDS) feature enables you to create point-to-point wireless links between two or more M330s. These links create a wireless bridge that interconnects the networks connected to the Ethernet port on each M330. For example, in the following figure, M330 #2 and M330 #3 use the WDS to create a wireless link between the main office network and a small network in a warehouse:



WDS links provide an effective solution for extending network coverage in situations where it is impractical or expensive to run cabling. Each M330 can create up to four WDS links.

Note

A network that includes WDS links should be distinguished from a group of clustered APs. WDS enables wirelessly extending the network, whereas clustering is used to simplify AP administration and optimize bandwidth use. See [“Clustering multiple M330s” on page 85](#) for more information.

Simultaneous AP and WDS support

The M330 simultaneously supports wireless communities and one or more WDS links. Although this offers flexibility, note that the total available bandwidth on the radio is shared between all WDS links and wireless users. This can result in reduced throughput if high volumes of traffic are being sent by both wireless users and the WDS links.

Using the 5 GHz band for WDS links

When the M330 uses WDS only to extend the network by providing a dedicated link to another M330 (that is, it does not simultaneously act as an AP for wireless clients), HP recommends that, whenever possible, the WDS links use 802.11a, 802.11n, or 802.11ac in the 5 GHz band. This optimizes throughput and reduces the potential for interference, as follows:

- Most Wi-Fi clients support 802.11b/g/n in the 2.4 GHz band, this frees the 5 GHz band for other applications such as WDS.
- Channels in the 5 GHz band are non-overlapping.
- Assuming an optimal implementation, 802.11a supports up to 54 Mbps, 802.11n supports up to 450 Mbps, and 802.11ac supports up to 1.3 Gbps, providing a fat pipe for traffic exchange.

Configuration considerations

The following guidelines apply when you create a WDS link between two or more M330s:

- The 5 GHz band has a shorter reach when compared to the 2.4 GHz band. This could be a factor depending on the distance your WDS link span.
- All radios configured for WDS must be set to the same channel. This means that on the **Wireless > Radio** page under **Channel**, you cannot select **Auto**.
- The Ethernet ports for all M330s must be connected to the same subnet, and each M330 must have a unique IP address.
- If WPA (PSK) security is enabled, the same link name and key must be defined on all M330s that are linked by the WDS connection.
- IEEE 802.11n uses frame aggregation, whereby multiple frames are combined into one to reduce overhead and increase throughput. WEP-encrypted frames are not aggregated, however, so enabling WEP security over WDS will result in reduced throughput.
- Although the M330 can support up to four WDS links, only one wireless link can be defined between any two M330s.

WDS configuration

To view or add a WDS link, select **Wireless > WDS**.

Configure WDS Bridges To Other Access Points

General

Spanning tree mode

☐ Enable ☒ Disable

WDS link 1

Radio

1

Local address

28:80:23:99:62:30

Remote address

Encryption

None (Plain-text)

WDS link 2

Radio

1

Local address

28:80:23:99:62:30

Remote address

Encryption

None (Plain-text)

WDS link 3

Radio

1

Local address

28:80:23:99:62:30

Remote address

Encryption

None (Plain-text)

WDS link 4

Radio

1

Local address

28:80:23:99:62:30

Remote address

Encryption

None (Plain-text)

Save

Cancel

General

Spanning tree mode

The Spanning-Tree Protocol (STP) can be enabled to prevent undesirable loops from occurring in the network that can result in decreased throughput. HP recommends that you enable spanning tree mode.

WDS link 1/2/3/4

You can link the M330 with up to four other M330 devices. Specify the following settings for each WDS interface:

Radio

Selects the wireless radio on the M330 for the WDS link: **Radio 1** for 2.4 GHz, and **Radio 2** for 5 GHz.

Local address

The MAC address of the default wireless community (SSID 0, the first SSID entry) on the selected M330 radio. The M330 only uses SSID 0 (the first SSID entry) on each radio to create the WDS link. This address needs to be entered as the **Remote address** on the M330 to which this link connects.

Remote address

Specify the MAC address of the default wireless community (SSID 0) on the remote M330 to which this link will connect. Or, click the left arrow next to the text box to select from a list of MAC addresses detected during an AP scan. The MAC address must be in the following format: six pairs of hexadecimal numbers, (including numbers 0 to 9 and letters a to f or A to F), with each pair separated by a colon. For example: 00:03:52:0a:0f:01.

Note

A common community name (SSID) is required on both APs to establish a WDS link. This SSID must be the first entry in the list of SSIDs on both APs (SSID 0 entry).

Encryption

Select how traffic exchanged between the two M330s will be encrypted.

The options are as follows:

- **None:** Data is transmitted unencrypted between M330 devices.
- **WEP:** Note that IEEE 802.11n uses frame aggregation, whereby multiple frames are combined into one to reduce overhead and increase throughput. WEP-encrypted frames are not aggregated, however, so enabling WEP security over WDS will result in reduced throughput.

Note

WEP cannot be used when the radio operating mode supports 802.11n or 802.11ac.

To enable WEP, configure the following settings:

- **Key length:** Select **64 bits** or **128 bits**.
- **Key type:** Select **ASCII** or **Hex**.
- **WEP key:** If you selected **ASCII**, enter any combination of 0 to 9, a to z, and A to Z, and special characters such as @ and #. If you selected **Hex**, enter hexadecimal digits (any combination of 0 to 9 and a to f or A to F). These are the RC4 encryption keys shared with the stations using the AP.
- **Confirm key:** Re-enter the key.
- **WPA (PSK):** Configure the following settings:
 - **Link name:** Enter a name for the new WDS link you have created. It is important that the same link name is entered at the other end of the WDS link. If this name is not the same for both APs on the WDS link, they will not be able to communicate and exchange data.

The name can be any alphanumeric combination.

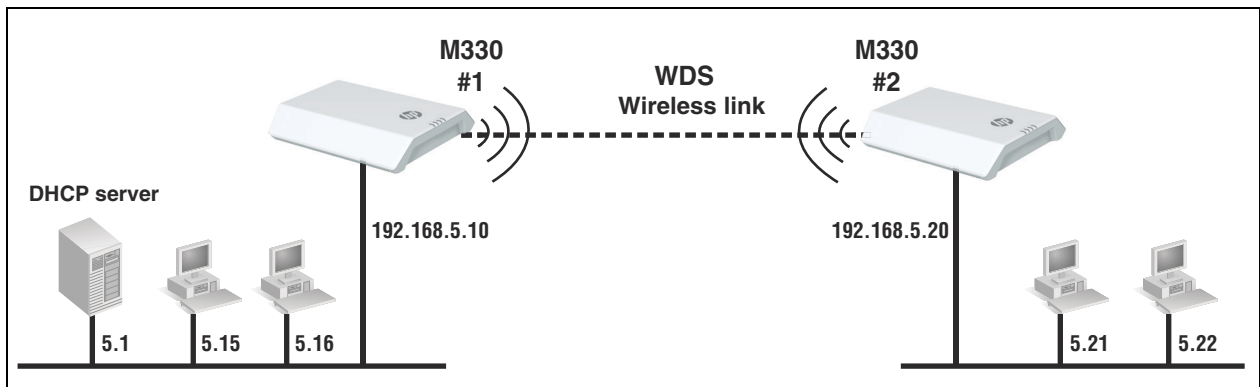
- **Key:** Enter a unique shared key for the WDS link. This unique shared key must also be entered for the AP at the other end of the WDS link. If this key is not the same for both APs, they will not be able to communicate and exchange data.

The WPA-PSK key uses AES encryption. It can be from 8 to 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. The key cannot begin with or end with spaces and cannot contain only spaces.

- **Confirm key:** Re-enter the key.

Example of a WDS Deployment

This example shows you how to create a wireless link between two physically separate network segments.



General Information

The following is assumed for the example provided:

- For initial configuration, M330 #1 and M330 #2 are both connected to the same switch and subnet. M330 #1 is installed on the main network. After configuration, M330 #2 serves a remote network.
- The switch is served by a DHCP server.

If no DHCP server is available, preconfigure each AP with a static IP address following the instructions provided in the *M330 Dual Radio 802.11ac Access Point Quick Start Guide*.

- Whether a dynamic or static address is assigned, it is necessary to determine the IP address of each AP. The IP address is required to launch the web-based management interface to configure each AP.

Note:

A WDS link that is successfully enabled between the two APs creates a loop on the switch. HP strongly recommends that you enable STP mode on both APs as described in this example.

Setting up a WDS link

To establish a WDS link, you must assign a common wireless community name (SSID) as the first entry in the list of SSIDs on both APs (SSID 0 entry). To configure an SSID, select **Wireless > Communities**. Select the radio and enter the **Network name** (SSID), for example, **WDS_330**. Repeat this step on the other AP using the same SSID.

For the APs to communicate, both APs must transmit and receive on the same channel. Select **Wireless > Radio**. Select the radio and select a channel that is unlikely to interfere with other devices in the nearby network. Repeat this step on the other AP.

Radio

Country
Country: US - United States

Basic settings

Radio: 2
 Status: ☒ On ☐ Off
 Mode: IEEE 802.11n/ac
 Channel: 36
 Channel bandwidth: 80 MHz
 Primary channel: Lower
 Current channel: 132 (5660 MHz)
 Station isolation: ☐

Advanced settings

Save Cancel

On M330 #1, select **Wireless > WDS**. Select the button to enable **Spanning tree mode**. Select the radio. The AP's MAC address for SSID 0 is prepopulated. Under **WDS link 1**, enter M330 #2's MAC address in the **Remote address** box. To discover M330 #2's MAC address, use one of the following options:

- If you are using radio 1, proceed to [Option 1 for radio 1 \(recommended\)](#).
- If you are using radio 2, proceed to [Entering the remote MAC address for radio 2 WDS configuration](#).

Option 1 for radio 1 (recommended)

On M330 #1, select **Wireless > WDS**. Under **WDS link 1**, click the left arrow next to the **Remote address** box. A list of SSIDs with their corresponding MAC address appears.

From the list, select the SSID of M330 #2. This populates the **Remote address** box with M330 #2's MAC address.

Repeat this step on the other AP (entering M330 #1's MAC address in M330 #2's **Remote address** box). Be sure to enable **Spanning tree mode** at the top of M330 #2 WDS page.

If the desired SSID is not on the list, proceed with Option 2.

Option 2 for radio 1 WDS deployment

On M330 #1, select **Home > System Summary**. The MAC address of M330 #1 is provided on the System Summary page.

Copy this MAC address, and then on M330 #2, select **Wireless > WDS** and paste the MAC address in the **Remote address** box.

Next, copy the MAC address of M330 #2 from the **System Summary** page, and paste it into the M330 #1 **Wireless > WDS** page **Remote address** box.

Now both APs can identify each other's MAC addresses on the common SSID.

If you are manually entering the MAC address, it must be in the following format: six pairs of hexadecimal numbers, (including numbers 0 to 9 and letters a to f or A to F), with each pair separated by a colon. For example: 00:03:52:0a:0f:01.

An unencrypted a WDS link is now established between the two APs.

To test the WDS link, disconnect M330 #2 from the switch. On M330 #1, select **Tools > Ping** and ping the address of M330 #2. If the ping succeeds, the WDS link is working.

Alternatively, connect a laptop to the Ethernet port of M330 #2, open a browser and browse the network. The remote AP provides network connectivity over the WDS link, if properly configured.

Proceed to Encrypting wireless traffic across the WDS link.

Setting up a WDS link on radio 2

Configuring a WDS network on radio 2 is similar to the process described for a radio 1 configuration with the following exception:

When configuring WDS on radio 2, you must select **Radio 2** in the Wireless Community, Radio, and WDS pages. By default, the radio setting is always radio 1.

Entering the remote MAC address for radio 2 WDS configuration

Option 1 (recommended)

On M330 #1, select **Wireless > WDS**. Under **WDS link 1**, click the left arrow next to the remote address box. A list of SSIDs with their corresponding MAC address appears.

From the list, select the SSID of M330 #2. This populates the **Remote address** box with M330 #2's MAC address.

Repeat this step on the other AP. Be sure to enable **Spanning tree mode** at the top of M330 #2's **Wireless > WDS** page.

In the event the desired SSID is not present in the list, proceed with Option 2 for radio 2 deployment.

Option 2 for Radio 2 WDS deployment

Each SSID on the AP has a unique MAC address. The first eight MAC addresses are assigned to SSID 0 through SSID 7 on radio 1. An additional eight MAC addresses are reserved for SSID 0 through SSID 7 on radio 2. All 16 SSID MAC addresses are in sequence and increment by 1 (hexadecimal).

On M330 #1, select **Home > System Summary**. The MAC address of M330 #1 is provided on the **System Summary** page. Write down this MAC address in the following format: six pairs of hexadecimal numbers, (including numbers 0 to 9 and letters a to f or A to F), with each pair separated by a colon. For example: 00:03:52:0a:0f:01.

Increment this address by 8. Note that MAC addresses are hexadecimal so you must use a hexadecimal calculator when adding 8 to the MAC address.

Go to the **Wireless > WDS** page of M330 #2 and enter this modified SSID address in the **Remote address** box.

Follow the same process to calculate the SSID MAC address M330 #2, and enter it in the **Remote address** box on the M330 #1 **Wireless > WDS** page.

An unencrypted a WDS link is now established between the two APs.

Encrypting wireless traffic across the WDS link

The AP offers WPA PSK to encrypt wireless traffic on the WDS link. HP recommends that you use encryption to secure traffic and the network. Each AP must be configured with the same WPA PSK passphrase.

WDS link 1	
Radio	2 ▾
Local address	28:80:23:99:62:38
Remote address	70:72:cfe3:71:50 ⓘ
Encryption	WPA (PSK) ▾
Link name	M330_WDS1 (1 - 32 characters)
Key (8 - 63 characters)
Confirm key

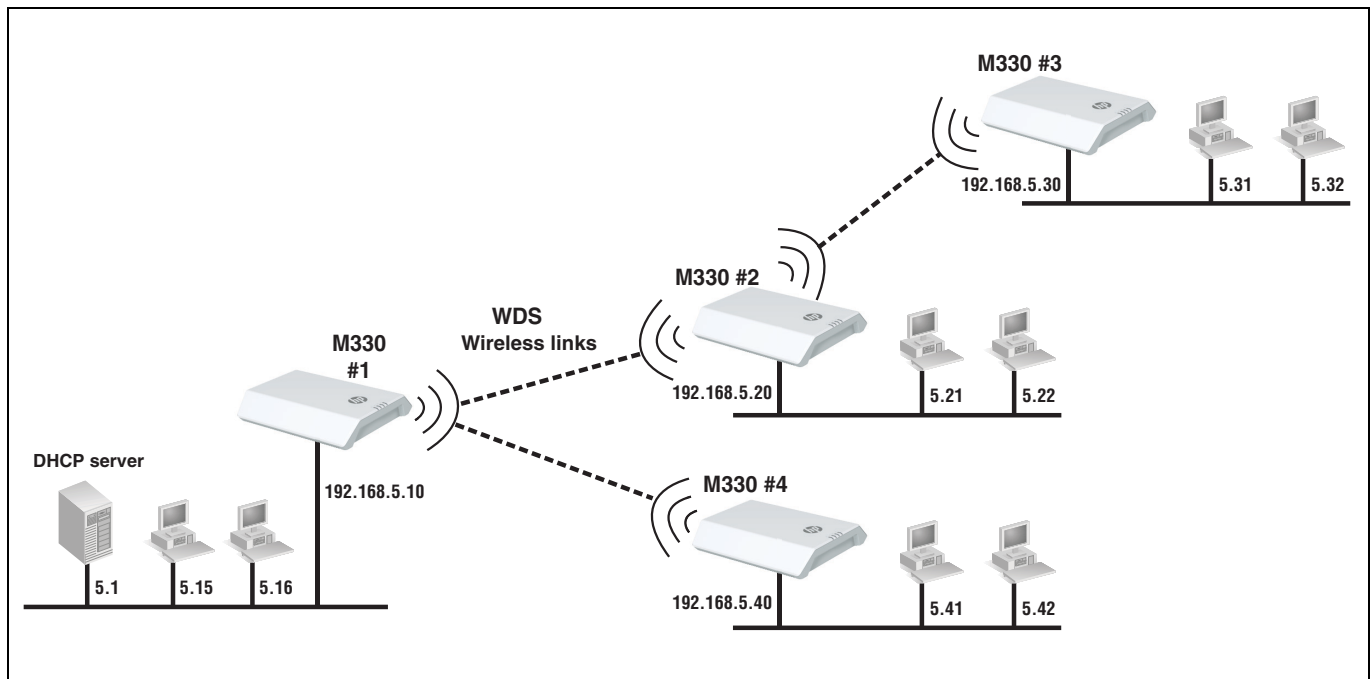
Enabling wireless encryption on a WDS link

Go to the **Wireless** > **WDS** page of either AP. Under **WDS link 1**, click the **Encryption** drop-down list, and select **WPA (PSK)**. You are now presented with additional fields:

- **Link name:** Enter a name for the WDS link that you created. It is important that the same link name is entered at the other end of the WDS link. If this name is not the same for both APs on the WDS link, they will not be able to communicate or exchange data. The name can be any alphanumeric combination.
- **Key:** Enter a shared key for the WDS link. This shared key must also be entered for the AP at the other end of the WDS link. If this key is not the same for both APs, they will not be able to communicate or exchange data. The WPA-PSK key uses AES encryption. It can be from 8 to 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. The key cannot begin with or end with spaces and cannot contain only spaces. Repeat this process on the other AP.

Multiple WDS link configuration

Similar to the single WDS wireless link example, up to four M330 access points can have WDS links to the same M330. The following example shows how to create multiple WDS links.



General Information

The following is assumed for the example provided:

- For initial configuration, M330 #1, M330 #2, M330 #3, and M330 #4 are all connected to the same switch and subnet. After completing configuration of all APs, M330 #1 is installed on the main network. After configuration, M330 #2, M330 #3, and M330 #4 serve remote networks.
- The switch is served by a DHCP server.

If no DHCP server is available, preconfigure each AP with a static IP address following the instructions provided in the *M330 Dual Radio 802.11ac Access Point Quick Start Guide*.
- Whether a dynamic or static address is assigned, it is necessary to determine the IP address of each AP. The IP address is required to launch the web-based management interface to configure each AP.

Note:

During the configuration process, WDS links that are successfully enabled between the APs creates a loop on the switch. HP strongly recommends that you enable STP mode on all APs.

Setting up multiple WDS links

The procedure for setting up multiple WDS links follows that for a single link. This example provides a summary of the procedure, for details of each step see [“Example of a WDS Deployment”](#) on page 69.

Set a common SSID

For each AP, select **Wireless > Communities**, and then select the radio and enter a **Network name** (SSID), for example, **WDS_330**.

Select a common operating channel

For the APs to communicate, all APs must transmit and receive on the same channel. For all APs, select **Wireless > Radio** and set the same channel for the selected radio.

Enable Spanning tree mode

For all APs, enable **Spanning tree mode** at the top of the **Wireless > WDS** page.

Enter WDS link remote MAC addresses

There are different options for setting up the WDS link remote MAC addresses (see [“Example of a WDS Deployment” on page 69](#)). Using the method you select, ensure the following addresses are configured:

- For M330 #1, configure the WDS link 1 **Remote address** with the MAC addresses of M330 #2, and the WDS link 2 **Remote address** with the MAC addresses of M330 #4.
- For M330 #2, configure the WDS link 1 **Remote address** with the MAC address of M330 #1, and the WDS link 2 **Remote address** with the MAC addresses of M330 #3.
- For M330 #3, configure the WDS link 1 **Remote address** with the MAC address of M330 #2.
- For M330 #4, configure the WDS link 1 **Remote address** with the MAC address of M330 #1.

Disconnect remote APs from the switch

Disconnect M330 #2, M330 #3, and M330 #4 from the switch and connect them to the networks at their remote locations.

Test the WDS links

To test the WDS links, select **Tools > Ping** on M330 #1 and ping the IP addresses of each remote AP. If the pings succeed, the WDS links are working.

Alternatively, connect a laptop to the network of each remote AP, open a browser and browse the network. The remote AP provides network connectivity over the WDS link, if properly configured.

Enable encryption for the WDS links

HP recommends that you use encryption on WDS links to secure traffic and the network. Both ends of each WDS link must be configured with the same WPA PSK passphrase. However, different WDS links can use different WPA PSK passphrases.

Go to the **Wireless > WDS** page of each AP. For each configured WDS link, click the **Encryption** drop-down list, and select **WPA (PSK)**. In the **Key** box, enter the same shared key for both ends of each WDS link.

For the **Link name**, enter the same link name at both ends of each WDS link. If this name is not the same for both APs on a WDS link, they will not be able to communicate or exchange data. The name can be any alphanumeric combination.

7 Configuring Ethernet, IP, and VLAN settings

Ethernet configuration

The M330 connects wireless clients to a wired network through its Ethernet port. You can configure the IP settings for this interface and the VLAN membership required for management access to the M330.

To configure the Ethernet port settings, select **Network > IP**.

Ethernet configuration	
MAC address	28:80:23:99:62:30
Management VLAN ID	<input type="text" value="1"/> (1 - 4094)
Untagged VLAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Untagged VLAN ID	<input type="text" value="1"/> (1 - 4094)

The **Ethernet configuration** area shows the **MAC address** assigned to the M330 Ethernet port and to the default wireless community (wlan0). The MAC address is also printed on the AP.

This page enables configuring the following settings:

Management VLAN ID

The management VLAN is VLAN 1 by default. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the M330 accordingly. The VLAN ID can be any value from 1 to 4094. Any management traffic received on a different VLAN is ignored.

Untagged VLAN Untagged VLAN ID

All traffic from wireless clients to the AP is associated with a VLAN ID. The VLAN ID may be assigned by a RADIUS server or determined by the client's association with a wireless community. Traffic between the wired network and the AP, however, might not be associated with a VLAN (that is, the traffic is untagged). These settings determine how the AP forwards untagged traffic to the wireless network.

If the **Untagged VLAN** option is enabled and an **Untagged VLAN ID** is specified:

- When the M330 receives traffic from a wireless client and that traffic has a VLAN ID that matches the **Untagged VLAN ID**, it forwards the traffic to the wired network with no VLAN tag.
- If the VLAN ID does not match the **Untagged VLAN ID**, the M330 forwards the traffic to the wired network with the VLAN ID from the wireless client.

If the **Untagged VLAN** option is disabled, all traffic that the M330 receives from a wireless client is forwarded to the wired network with the same VLAN tag it used on the wireless network.

The M330 does not add VLAN tags when forwarding traffic to wireless clients, regardless of whether the traffic was tagged or untagged on the wired network.

By default, this option is enabled and the untagged VLAN ID is 1.

Note

If VLANs are not used on your network, these settings have no effect on the forwarding of traffic.

IPv4 configuration

Use this area to configure the M330 to be assigned an IPv4 address from a DHCP server on your network, or to statically configure an IPv4 address.

Automatically assigning an IP address (default method)

By default, **Connection type** is set to **DHCP** and the M330 operates as a DHCP client. This means that if the network has a DHCP server, the M330 will automatically receive a new IP address in place of its default IP address (192.168.1.1) upon connecting to the network.

The DHCP server will assign an address from its pool of available addresses. You can find the IP address of the M330 by looking for its Ethernet base MAC address in the DHCP server log. The Ethernet MAC address is printed on the M330 label identified as **Ethernet Base MAC**, or listed on the management tool *IP* page as **MAC address**.

To have the DHCP server assign a specific IP address to the M330, you need to preconfigure the DHCP server to associate the IP address you want to use with the MAC address of the Ethernet port on the M330.

Static IP configuration

You can manually assign an IP address to the Ethernet port. This requires that you also define the address of the default gateway and DNS server that are in use on your network.

To configure a static IP address, select **Network** > **IP** and configure the following fields:

IPv4 configuration	
Connection type	Static IP ▾
Static IP address	192 . 168 . 1 . 1
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 1 . 254
DNS nameservers	<input type="radio"/> Dynamic <input checked="" type="radio"/> Manual
	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Connection type

Select **Static IP** from the list to manually configure an IPv4 Ethernet address.

IP address

Set an address that is on the same subnet as the network to which the M330 will connect once installed. Respect any DHCP server-mandated static address ranges.

Subnet mask

Specify the mask for the IP address.

Default gateway

Set the IP address of the gateway on the network.

DNS nameservers:

Select **Dynamic** to have the DNS nameservers assigned through DHCP, or select **Manual** to configure up to two static DNS nameserver addresses.

IPv6 configuration

If the attached network uses the IPv6 protocol, you can enable IPv6 support on the M330. IPv6 functionality is enabled by default.

To configure IPv6 functionality, select **Network** > **IP** and configure the following fields:

IPv6 configuration	
IPv6	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPv6 connection type	DHCPv6 ▼
Static IPv6 address	<input type="text"/>
Static IPv6 address prefix length	<input type="text" value="0"/> (0 - 128)
Default IPv6 gateway	<input type="text"/>
Static IPv6 address status	
IPv6 link local address	fe80::2a80:23ff:fe99:6230/64
IPv6 auto config	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPv6 autoconfigured global addresses	
IPv6 DNS Nameservers	<input checked="" type="radio"/> Dynamic <input type="radio"/> Manual
	<input type="text"/>
	<input type="text"/>

IPv6

Enable or disable the ability to use IPv6 addressing to access the web user interface for AP configuration. This setting does not enable or disable IPv6 functionality on the network itself.

IPv6 connection type

Select **Static IPv6** from the list to manually configure an IPv6 address, or leave the default setting of **DHCPv6** for automatic IPv6 address assignment.

Static IPv6 address

The AP can have a static IPv6 address even if addresses have already been configured automatically. Enter an address in the form XXXX:XXXX:XXXX:XXXX.

Static IPv6 address prefix length

The prefix length must be an integer in the range from 0 to 128. The prefix length determines the part of the IPv6 address that identifies the network that the M330 is attached to.

Default IPv6 gateway

The default gateway address for IPv6 traffic destined outside the network.

Static IPv6 address status

The operational status of the static IPv6 address assigned to the M330 management interface. The possible values are as follows:

- **Operational:** The IP address has been verified as unique on the LAN and is usable on the interface.
- **Tentative:** The M330 initiates a duplicate address detection (DAD) process automatically when a static IP address is assigned. An IPv6 address is in the tentative state while it is

being verified as unique on the network. While in this state, the IPv6 address cannot be used to transmit or receive traffic, except to exchange messages with other network nodes to verify the uniqueness of the address.

- **Blank (no value):** No IP address is assigned or the assigned address is not operational.

IPv6 link local address

The IPv6 link local address is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.

IPv6 auto config

When IPv6 auto configuration is enabled, the M330 processes the Router Advertisements received on the LAN port to determine its IPv6 addresses. The M330 can have multiple autoconfigured IPv6 addresses. The autoconfigured addresses coexist with the statically configured address. The AP can be accessed using either the statically configured or the automatically obtained IPv6 address.

IPv6 autoconfigured global addresses

If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed.

IPv6 DNS nameservers

Select **Dynamic** to have the IPv6 DNS servers assigned through DHCPv6, or select **Manual** to configure up to two static IPv6 DNS server addresses.

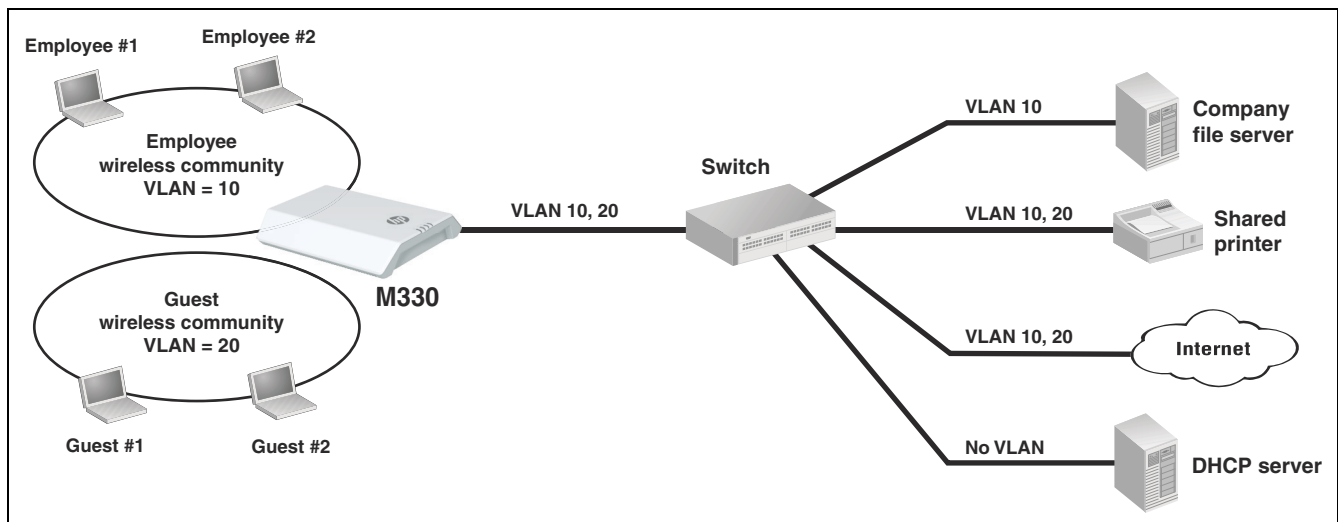
VLAN configuration

When the AP receives traffic from a wireless client, the AP may forward it on the Ethernet network to which the AP connects. Client traffic may be associated with a VLAN as it is forwarded to the Ethernet network.

VLAN assignment via wireless communities

The easiest way to assign user traffic to a VLAN is to configure the **VLAN ID** setting in a wireless community (See “[Wireless community configuration options](#)” on page 32). This puts all the traffic from users that connect to the wireless community onto the specified VLAN via the M330 Ethernet port.

In the following scenario, two wireless communities are defined, each with its own VLAN:



- The Employee wireless community is configured with VLAN 10. All employee traffic exits the M330 on VLAN 10, providing access to the company file server, shared printer, and the Internet.
- The Guest wireless community is configured with VLAN 20. All traffic from the Guest community exits the M330 on VLAN 20, providing access to the shared printer and the Internet.

VLAN assignment via RADIUS

VLANs can also be assigned on a per-user basis by setting VLAN attributes in a user's RADIUS account. To use this option, you need to do the following:

- Configure a wireless community with **Security method** set to **WPA Enterprise** or **IEEE802.1X**. For configuration details, see ["Wireless protection" on page 33](#).
- Configure the RADIUS server information for the selected security type.
- On the RADIUS server, configure user accounts with the appropriate VLAN attributes.

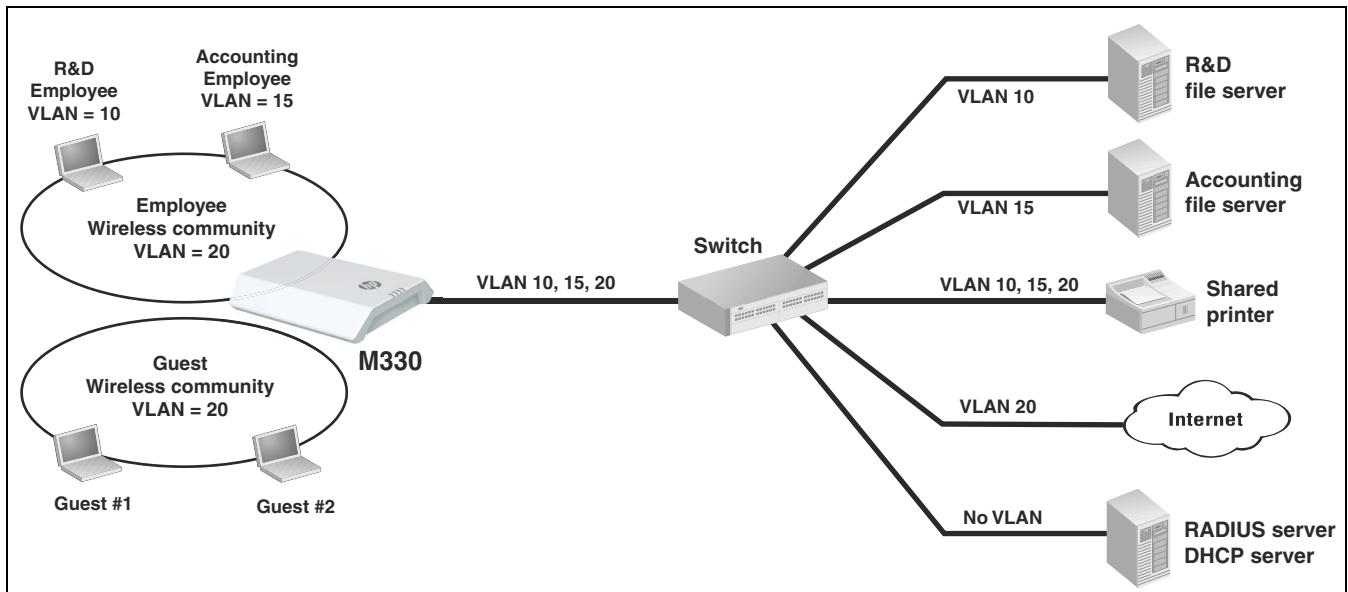
Note

When a VLAN is defined in a user's RADIUS account, it always overrides the VLAN defined for a wireless community. This enables you to define an VLAN setting for a community and then override it on a per-user basis as required.

RADIUS-assigned VLANs are created and deleted dynamically as clients associate and disassociate with the M330. When the first client assigned by RADIUS to a particular VLAN authenticates with the M330, the M330 creates the VLAN. When the last client using that VLAN disassociates, the VLAN is deleted from the M330. The maximum number of dynamic VLANs is equal to the maximum number of configurable clients on the AP.

Example

In the following scenario, RADIUS user accounts are configured to assign employees to different VLANs depending on the workgroup to which an employee belongs:



Employee wireless community

- R&D employees are assigned to VLAN 10 via attributes in their RADIUS account.
- Accounting employees are assigned to VLAN 15 via attributes in their RADIUS account.
- Employees without a VLAN assignment in their RADIUS account get assigned to the VLAN that is configured for the wireless community, which in this example is 20. This enables these employees to access the shared printer and the Internet.

Guest wireless community

- The Guest community does not use RADIUS. All traffic on the Guest community is assigned to VLAN 20, providing access to the shared printer and the Internet.

Port statistics

To view statistics on Ethernet/WDS packets received and transmitted on the wired and wireless ports, select **Status > Ports**. The port statistics page displays.

Ports							
Ethernet statistics							
Radio		1 ▾					
Status	Port	Receive			Transmit		
		Packets	Dropped	Errors	Packets	Dropped	Errors
up	Port 1	4579	0	0	4259	0	0
up	Community 0	0	0	0	513	0	0
down	Community 1	0	0	0	0	0	0
down	Community 2	0	0	0	0	0	0
down	Community 3	0	0	0	0	0	0
down	Community 4	0	0	0	0	0	0
down	Community 5	0	0	0	0	0	0
down	Community 6	0	0	0	0	0	0
down	Community 7	0	0	0	0	0	0
WDS statistics							
Status	Port	Receive			Transmit		
		Packets	Dropped	Errors	Packets	Dropped	Errors
down	WDS interface 1	0	0	0	0	0	0
down	WDS interface 2	0	0	0	0	0	0
down	WDS interface 3	0	0	0	0	0	0
down	WDS interface 4	0	0	0	0	0	0
							Refresh

Select **Radio 1** or **Radio 2** to view traffic accumulated on wireless communities and on WDS interfaces. The statistics accumulate until the AP is rebooted.

Port

The LAN port is listed as Port 1. The Wireless port entry includes all wireless communities and WDS interfaces, even when not configured.

Packets

The total number of packets received or transmitted on the interface.

Dropped

The number of packets dropped upon receipt or transmission.

Errors

The number of packets received or transmitted that had errors.

8 Clustering multiple M330s

Overview

The M330 supports AP clustering. A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity rather than a series of separate wireless devices. When APs are clustered, you can also configure channel planning, which helps to reduce radio interference and maximize bandwidth on the wireless network.

The AP cluster is a dynamic, configuration-aware group of APs in the same subnet of a network. Each cluster can have up to 16 members. Only one cluster per wireless network is supported; however, a network subnet can have multiple clusters. Clusters can share various configuration settings, such as VSC settings and QoS queue parameters.

Shared settings in a cluster

When clustering is enabled, some configuration items are shared by the entire cluster, and other items remain unique to each M330. In the management tool, an icon displays next to items that are shared. When clustering is disabled, the icon does not display.

System Time ?

Set system time

System time (24 HR) ⓘ Tue Jan 1 2013 12:40:36 PST

Set system time ⓘ ☐ Using network time protocol (NTP)

☒ Manually

System date January 1 2013

System time (24 HR) 12 : 40

Time Zone ⓘ USA (Pacific)

Adjust time for daylight saving

Enable ⓘ ☒

DST start (24 HR) ⓘ Second Sunday in March at 02 : 00

DST end (24 HR) ⓘ First Sunday in November at 02 : 00

DST offset (minutes) ⓘ 60

Save **Cancel**

Settings that are shared/not shared by the cluster

Settings that are shared	Settings that are not shared
System Log settings	WDS links
Rogue AP Detection	Ethernet (wired) settings
Wireless settings (Exception: Static channel configuration is not shared.)	Radio settings:
Network Time Protocol (NTP), time, and daylight savings time settings	<ul style="list-style-type: none">• Channel• Beacon interval• DTIM period• Transmit power
Radio settings, as follows:	Country setting
<ul style="list-style-type: none">• Status• Mode• Channel bandwidth• Primary channel• Station Isolation• Multidomain regulatory mode• Short guard interval supported• STBC mode• Protection• Fragmentation threshold• RTS threshold• Fixed multicast rate• Broadcast/multicast rate limiting	Network trace
Wireless community settings	Settings collected in the showtech.rtf and showdev.out files.
MAC authentication	Developer info collection
Basic SNMP settings	
Channel planning	
Admin password to secure any new cluster members	
Email alert settings	
Captive Portal	
Management settings	

IPv4 and IPv6 clusters

The M330 supports IPv4 and IPv6 mode clusters.

Cluster formation

Cluster criteria

A cluster can be formed between two or more M330 APs if the following conditions are met:

- All M330 APs in the cluster must have the same part number. Different regional models cannot be mixed in the cluster. You can view the part number on the **System Summary** page.
- The APs are configured with the same **Country** setting.
- The APs are connected on the same wired subnet. Clustering is not supported over a wireless connection such as a WDS link.
- The APs joining the cluster have the same **Cluster name** setting.
- The APs are configured with the same **Cluster IP version** setting (IPv4 or IPv6).
- Clustering is enabled on each AP.

Cluster negotiation

When an M330 is configured with a cluster name and clustering is enabled, it begins sending periodic advertisements every 10 seconds to announce its presence. If there are other M330s that match the criteria for the cluster, arbitration begins to determine which AP provides its configuration to the others. The first AP to advertise itself as a member of the cluster wins the arbitration.

The following rules apply to cluster formation:

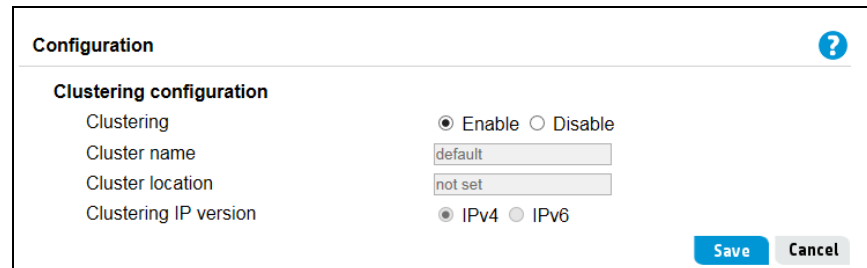
- For existing clusters, whenever the administrator updates the configuration of any member of the cluster, the configuration change is shared with all members of the cluster, and the configured AP assumes control of the cluster.
- When two separate clusters join into one, then the cluster that was created first wins arbitration for cluster control. The configuration on the newly formed cluster is overwritten by the configuration on the new cluster controller.
- If a cluster does not receive cluster advertisements from an AP for more than 60 seconds (when, for example, the AP loses connectivity to other APs in the cluster), the AP is removed from the cluster.
- If a clustered AP loses connectivity, it is not immediately dropped from the cluster. If it regains connectivity and rejoins the cluster without having been dropped, and configuration changes were made to that AP during the lost connectivity period, the changes will be propagated to the other cluster members when connectivity resumes.
- If a clustered AP loses connectivity, is dropped from the cluster, and later rejoins the cluster, and configuration changes were made in the cluster during the lost connectivity period, the

changes will be propagated to the AP when it rejoins. If there are configuration changes in both the disconnected AP and the cluster, then the AP with the greatest number of changes and, secondarily, the most recent change, will be selected to propagate its configuration to the cluster. (That is, if AP1 has more changes, but AP2 has the most recent change, AP1 is selected. If they have an equal number of changes, but AP2 has the most recent change, then AP2 is selected.)

Creating a cluster

To create a cluster:

1. On the first M330 that you want to be clustered, select **Cluster > Configuration**.



The screenshot shows the 'Configuration' page with a 'Clustering configuration' section. It includes radio buttons for 'Enable' (selected) and 'Disable'. Below are text input fields for 'Cluster name' (containing 'default') and 'Cluster location' (containing 'not set'). At the bottom, there are radio buttons for 'IPv4' (selected) and 'IPv6'. 'Save' and 'Cancel' buttons are at the bottom right.

2. For the **Clustering** mode, select **Enable**.
3. Enter a **Cluster name** (required). The cluster name must be the same on all APs. It can consist of up to 64 alphanumeric and special characters.
4. Enter a **Cluster location**, which describes where the AP is physically located. This setting is used for information purposes only.
5. Select a **Cluster IP version**.

All members of a cluster must have the same IP version (**IPv4** or **IPv6**).

If you choose **IPv6**, clustering can use the link local address, autoconfigured IPv6 global address, and statically configured IPv6 global address. Ensure that when using IPv6 for clustering all the APs in the cluster either use link-local addresses only or use global addresses. Clustering will not work with mixed address versions.

6. Select **Save**.

The M330 begins searching for other APs in the subnet that are configured with the same cluster name and IP version. A potential cluster member sends advertisements every 10 seconds to announce its presence.

A **Cluster members** area displays a single entry for this AP if this is a newly created cluster. If the cluster already exists, information on each cluster member displays in a table.

7. Repeat steps 1 to 6 on each of up to 15 additional APs that you want to join the cluster.

As subsequent APs are configured with the same clustering information, the **Cluster members** area displays a table with IP and other information for each cluster member.

Cluster members		
IP address	MAC address	Location
192.168.1.1	28:80:23:99:62:30	not set

Removing an AP from the cluster

To remove an AP from the cluster:

1. On the M330 that you want to remove from the cluster, select **Cluster > Configuration**.
2. For the Clustering setting, select **Disable**, then select **Save**.

Client connections

From any AP in a cluster, you can select **Cluster > Client connections** to view information about clients connected to any clustered AP.

Note

This page displays data only if clustering is enabled on the **Cluster > Configuration** page.

Client Connections ?							
Client connections status							
AP MAC	User MAC	Idle	Rate (Mbps)	Signal	Rx total	Tx total	Error rate

Information shown in tables can be sorted by selecting the desired column label.

Note

This page shows a maximum of 20 clients on each clustered AP. To see all clients associated with a particular AP, view the **Wireless > Client connections** page directly on that AP.

AP MAC

Media Access Control (MAC) address of the AP.

The address shown here is the MAC address for the Ethernet interface and the default wireless community (wlan0). This is the address by which the AP is known externally to other networks.

User MAC

The Media Access Control (MAC) address of the client.

Idle

The time in seconds that has elapsed since the last client activity.

Rate (Mbps)

The speed in Mbps at which this AP is transferring data to the specified client. This value should fall within the range of the advertised rate set for the mode in use on the AP. For example, 6 to 54 Mbps for 802.11a.

Signal

The strength of the radio frequency (RF) signal the client receives from the AP.

This measurement is known as Received Signal Strength Indication (RSSI), which is indicated by a value ranging from 0 to 100. RSSI is determined by a mechanism implemented on the wireless interface of the client.

Rx total

The number of total packets received by the client during the current session.

Tx total

The number of total packets transmitted to the client during the current session.

Error rate

The percentage of time frames are dropped during transmission to or from this client.

Channel planning

When channel planning is enabled, the M330 automatically assigns radio channels used by clustered APs. Automatic channel assignment reduces mutual interference (or interference with other APs outside of its cluster) and maximizes Wi-Fi bandwidth to help maintain the efficiency of communication over the wireless network.

You must start channel planning to get automatic channel assignments. It is disabled by default.

At a specified interval, the channel manager maps APs to channel use and measures interference levels in the cluster. If significant channel interference is detected, the channel manager automatically reassigns some or all of the APs to new channels according to an efficiency algorithm (or automated channel plan). If the channel manager determines that a change is necessary, it sends the new channel assignments to all members of the cluster and generates a syslog message that indicates the sender AP and the new and old channel assignments.

The **Cluster > Channel planning** page shows current and planned channel assignments for clustered APs. You can start channel planning to optimize channel usage across the cluster on a scheduled interval.

Note

This page displays channel planning fields only if clustering is enabled on the **Cluster > Configuration** page.

Stopping/Starting Automatic Channel Assignment

By default, automatic channel planning is disabled (off).

Note

Channel planning overrides the default cluster behavior, which is to synchronize radio channels of all APs across a cluster. When Channel planning is enabled, the radio channel is not synced across the cluster to other APs.

Click **Enable** to resume automatic channel planning. When automatic channel planning is enabled, the Channel Manager periodically maps radio channels used by clustered access points and, if necessary, re-assigns channels on clustered APs to reduce interference (with cluster members or other APs outside the cluster).

Click **Disable** to stop automatic channel planning. (No channel usage maps or channel re-assignments will be made. Only manual updates will affect the channel assignment.)

Note

When automatic channel planning is enabled, the channel policy for the radio is automatically set to static mode, and the **Auto** option is not available for the **Channel** field on the Wireless Settings or Radio pages. This allows the automatic channel feature to set the channels for the radios in the cluster.

Configuration

Use this section to enable channel planning and configure basic settings.

Channel Planning ?

Channel planning configuration

Channel planning ⓘ

☐ Enable ☒ Disable

Channel change interval ⓘ

1 Hour ▼

Interference threshold ⓘ

75% ▼

Last proposed set of channel assignments

Save

Cancel

Channel planning

Enable or disable channel planning. It is disabled by default.

Channel change interval

Select the schedule for automated updates. At the selected interval, channel usage is reassessed and the resulting channel plan is applied. A range of intervals is provided, from 30 minutes to 6 months. The default is 1 hour.

Interference threshold

Select the minimum percentage of interference reduction a proposed plan must achieve to be applied. The default is 75 percent. You can select percentages ranging from 5 percent to 75 percent.

This setting lets you set a gating factor for channel reassignment so that the network is not continually disrupted for minimal gains in efficiency.

For example, if channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce interference by 30 percent, then channels will not be reassigned. However, if you reset the minimal channel interference threshold to 25 percent, the proposed channel plan will be implemented and channels will be reassigned as needed.

Last proposed set of channel assignments

If a channel plan was previously applied on the AP, this field shows the number of hours and minutes that have passed since it was applied.

Current channel assignments

Use this section to view the list of all APs in the cluster by IP address. The display shows the band on which each AP is broadcasting (a/b/g/n/ac), the channel currently used by each AP, and an option to lock an AP on its current radio channel so that it cannot be reassigned to another.

Current channel assignments						
IP address	Radio	Band	Channel	Proposed channel	Status	Locked
192.168.1.1	28:80:23:99:62:38	A/N/AC	36		up	<input type="checkbox"/>
192.168.1.1	28:80:23:99:62:30	B/G	6		up	<input type="checkbox"/>

Save

IP address

The AP IP address.

Radio

The MAC address of the radio.

Band

The band on which the AP is broadcasting.

Channel

The radio channel on which this AP is broadcasting.

Proposed channel

The channel to which this AP will be reassigned when the current channel plan is applied. The proposed channel and current channel can be different if any of the following have occurred:

- Dynamic Frequency Selection (DFS) is enabled and has marked the proposed channel out-of-service.
- The channel is locked because the **Locked** checkbox is selected.
- The proposed channel has not yet been applied (there is a small window of time between the proposal and the application of the proposed channel).

Status

Indicates whether the channel is up or down.

Locked

You can select to lock the AP onto the current channel. When selected, automated channel plans cannot reassign the AP to a different channel as a part of the optimization strategy. Instead, APs with locked channels will be factored in as requirements for the plan.

9 Captive portal

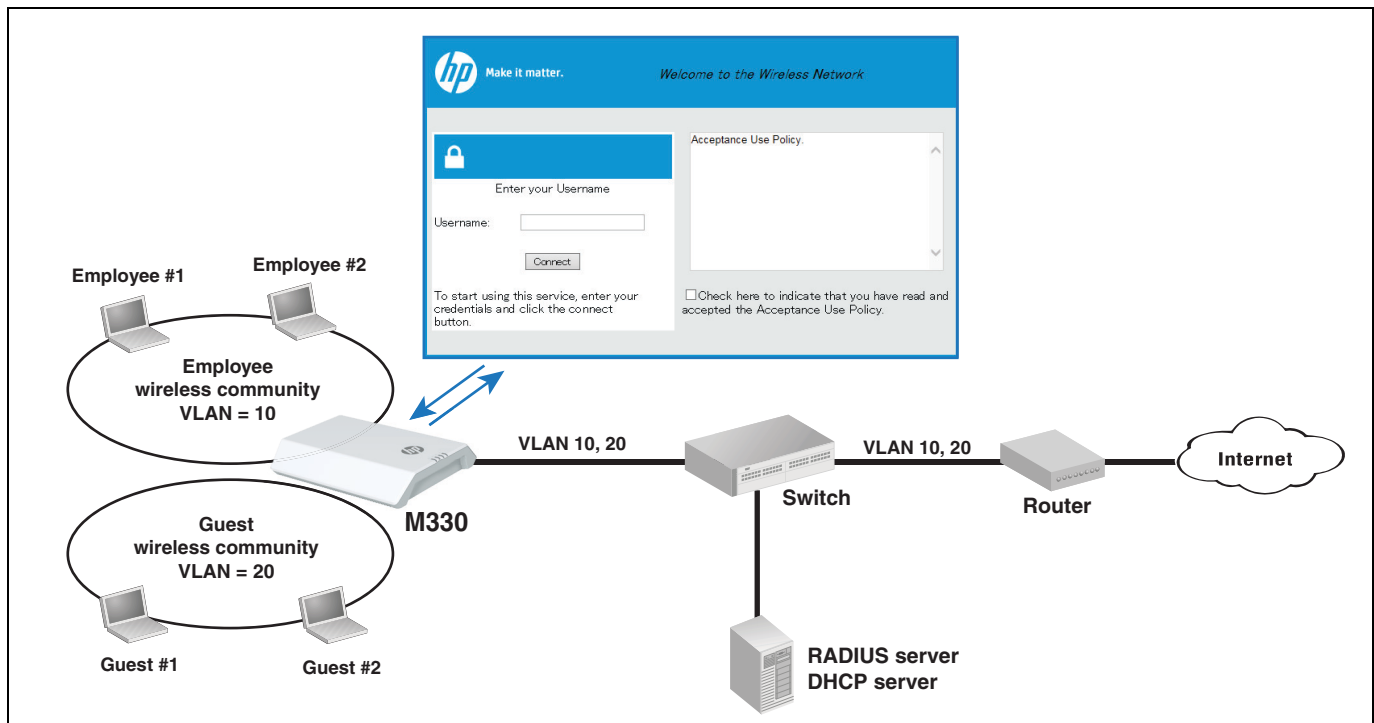
Overview

Captive Portal is a feature that blocks wireless clients from accessing the network until user verification has been established. The captive portal verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted. The database can be stored locally on the M330 or on a RADIUS server.

A captive portal is often used for public access networks, providing simple user name and password authentication through a web page log on. Even for guest users that do not require authentication, the Captive Portal web page can offer a number a benefits:

- Identify the wireless network and prevent users from logging on to rogue networks
- Provide terms of use policies for users to accept
- Provide additional information for users
- Restrict bandwidth for users to prevent network abuse

The following topology illustrates a basic captive portal configuration for both employee and guest access to a wireless network. Two wireless communities are configured for the employee and guest users. The employee community is assigned to VLAN 10 and the guest community assigned to VLAN 20.



A guest user can associate with the AP, but cannot initially access the network. When a guest attempts to access the Internet, a captive portal web page for guest users displays and the user must first accept the terms of use policy and optionally enter a user name. Once connected to the network, the guest user traffic is restricted to VLAN 20 and only has access to the Internet.

When an employee attempts to access the network, a different captive portal web page for employee users displays. An employee logs in using their user name and password and is first authenticated before being granted access to the network. The employee user traffic is tagged as VLAN 10, which provides access to the Internet and other network resources.

Setting-up captive portal

Setting-up captive portal on the M330 involves these basic steps:

1. Decide how you want to group the wireless users for login purposes. The M330 supports up to two captive portal instances. Each captive portal instance can be configured with one of three verification types as follows:

- Guest: No authentication but user must accept terms of use.
- Local: User authentication based on a list of users stored on the AP.
- Radius: User authentication based on an external RADIUS server.

It is common to configure a Guest captive portal instance for unauthenticated guests (Verification set to **Guest**) and a second captive portal instance for authenticated users (Verification set to either **Local** or **RADIUS**).

2. Enable the captive portal feature and set global parameters. See [“Basic configuration” on page 95](#).
3. Create and configure a captive portal instance.

A captive portal instance defines how a group of users are authenticated. The AP supports two captive portal instances. See [“Advanced configuration” on page 96](#).

4. Bind captive portal instances to wireless communities. Typically, authorized users are assigned to a different captive portal instance and wireless community than guest users. See [“Community binding” on page 100](#).

To assign VLANs to wireless communities, see [“VLAN configuration” on page 80](#).

5. Create a web locale and associate it to a captive portal instance.

A web locale is a customized captive portal authentication web page. Up to three locales can be created and associated with a captive portal instance, which enables the display of captive portal pages in multiple languages (up to three). The language of choice can be selected from the upper left-hand side of the main captive portal page. See [“Web customization” on page 101](#).

6. Create captive portal user accounts and user groups. Up to 128 users can be configured in the local database. See [“Local user/group association” on page 106.](#)

For a step-by-step walk-through of the configuration process, see [“Example of guest captive portal configuration” on page 110.](#)

Basic configuration

Use the Basic Configuration page to control the administrative state of the captive portal feature and configure global settings that affect all captive portal instances configured on the AP.

To configure basic captive portal features, select **Captive Portal** > **Basic Configuration**. The Basic Configuration page displays.

The following parameters are on the Basic Configuration page.

Captive Portal mode

Enables or disables the administrative mode of the captive portal on the AP.

Authentication timeout

To gain network access through a captive portal, clients are directed to an authentication web page where they must first enter authentication information. This parameter is the maximum number of seconds an authentication session remains open for a wireless client before the session is terminated. A session is terminated when a client does not enter valid credentials on the authentication WEB page within the timeout period. The authentication timeout range is 60-600 seconds, and the default is 300 seconds.

Additional HTTP port

Typically, HTTP traffic uses port 80, but an additional port can be configured. Specify a port number between 1025 and 65535, or port 80. The HTTP and HTTPs ports cannot be the same.

Additional HTTPS port

Typically, HTTP traffic over SSL (HTTPS) uses port 443, but an additional port can be configured. Specify a port number between 1025 and 65535, or port 443. The HTTP and HTTPs ports cannot be the same.

Instance count

The number of captive portal instances currently configured on the AP. The AP supports up to two instances.

Group count

The number of captive portal groups currently configured on the AP. The AP supports up to three groups including the default group. The default group cannot be deleted.

User count

The number of captive portal users currently configured on the AP. The AP supports up to 128 users.

Advanced configuration

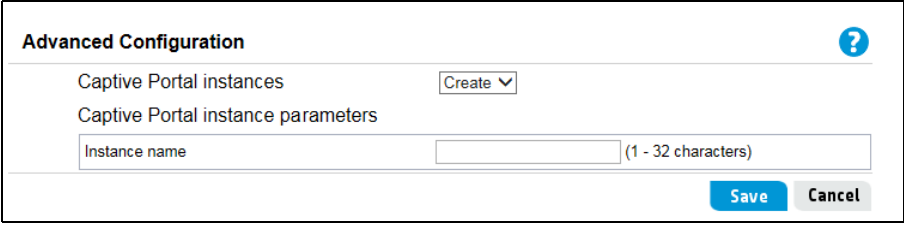
A captive portal instance is a defined set of parameters that can be associated with one or more wireless communities. This enables the AP to respond differently to certain users when they access the network community. The AP supports up to two instances.

Creating a captive portal instance

The AP has no captive portal instances configured by default. To create an instance, you must first assign a name to the instance, and then click **Save**.

The AP supports two instances. If both instances are already configured, you must first delete an instance before you can create a new one.

To create a captive portal instance, select **Captive Portal > Advanced Configuration**. The Advanced Configuration page displays.



The screenshot shows a web interface titled "Advanced Configuration" with a help icon (question mark) in the top right corner. Below the title, there are two sections: "Captive Portal instances" and "Captive Portal instance parameters". The "Captive Portal instances" section contains a "Create" button with a dropdown arrow. The "Captive Portal instance parameters" section contains a text input field labeled "Instance name" with a placeholder "(1 - 32 characters)". At the bottom right of the form, there are "Save" and "Cancel" buttons.

For **Captive Portal instances**, select **Create** and enter a name of 1-32 characters in the **Instance name** field. Click **Save** to create the instance. The **Captive Portal instance parameters** are then displayed and can be configured.

Configuring a captive portal instance

The captive portal instance parameters displayed on the Advanced Configuration page depend on the **Verification** setting. The AP supports the following three methods for client verification:

- **Guest:** Users are not authenticated.
- **Local:** Verifies client access against a database of authorized users on the AP.
- **Radius:** Verifies client access against a database of authorized users on a RADIUS server.

Guest verification

The following fields are displayed on the Advanced Configuration page when **Verification** is set to **Guest**.

The screenshot shows the 'Advanced Configuration' window for a Captive Portal instance named 'TestCP1'. The 'Captive Portal instance parameters' section is expanded, showing the following settings:

Parameter	Value	Range/Options
Instance ID	1	
Admin mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Protocol	http	
Verification	Guest	
Redirect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Redirect URL		(0 - 256 characters)
Away time	60	(0 - 1440 min)
Session timeout	0	(0 - 1440 min)
Max bandwidth upstream	0	(0 - 1300 Mbps)
Max bandwidth downstream	0	(0 - 1300 Mbps)
Locale count	0	
Delete instance	<input type="checkbox"/>	

At the bottom right of the configuration window are 'Save' and 'Cancel' buttons.

Captive Portal instances

Select an existing instance to view or configure its settings, or select **Create** to configure a new captive portal instance. The AP supports two instances. If both instances have been configured, you must delete an instance before you can create a new one.

Instance ID

The captive portal instance identifier. For an existing instance, this field cannot be configured. When creating a new captive portal instance, the ID cannot be used by another captive portal instance.

Admin mode

Click the option to enable or disable the administrative mode of the selected instance.

Protocol

Specifies HTTP or HTTPS as the protocol for the captive portal instance to use during the verification process.

Verification

The method used to authenticate clients. Select **Local** to use a database of authorized users on the AP, or select **Radius** to use a RADIUS server. If **Guest** is selected, users are not authenticated.

Redirect

Select Enable to redirect newly authenticated clients to a configured URL. When disabled, the locale-specific welcome page is displayed for clients.

Redirect URL

The URL for redirected clients. This can be either an IPv4 or IPv6 address. The IPv4 address should be in a form similar to http://xxx.xxx.xxx.xxx (http://192.168.1.10). The IPv6 address should be in a form similar to http://[xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (http://[2001:DB8::36A5:1C32]). One double colon may be used in the IPv6 address to indicate the appropriate number of zeros required to fill the undefined fields.

Away time

The time that a client entry is retained in the captive portal authenticated client list after it has disassociated from the AP. Specify a time between 0 and 1440 minutes. The default setting is 60 minutes.

Note

Each user also has a configured **Away time** setting. See the **Local User/Group Association** page. The local user timeout value has precedence over the captive portal instance value configured on this page.

Session timeout

The amount of time to wait before terminating a session. A user is logged out after the session timeout expires. If the value is set to 0, the timeout is disabled. Specify a time between 0 and 1440 minutes. The default value is 0.

Max bandwidth upstream

The maximum speed at which a client can send data to the network when using the captive portal. Specify a value between 0 and 1300 Mbps. The default value is 0, which means that no limit is enforced.

Max bandwidth downstream

The maximum speed at which a client can receive data from the network when using the captive portal. Specify a value between 0 and 1300 Mbps. The default value is 0, which means that no limit is enforced.

Locale count

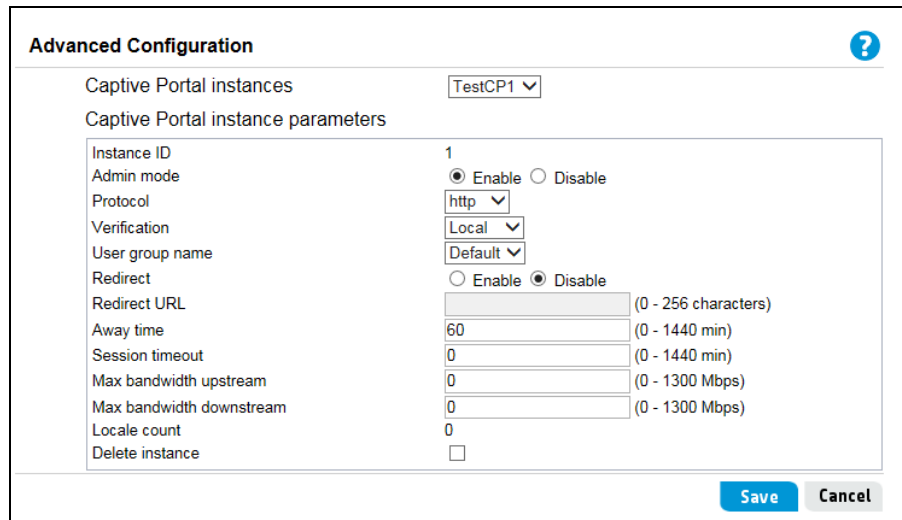
The total number of locales that are associated with this instance. Up to three locales are supported for each captive portal instance, as assigned on the Web Customization page.

Delete instance

To delete the current instance, select this option and click **Save**.

Local verification

The following additional field is displayed on the Advanced Configuration page when **Verification** is set to **Local**.



The screenshot shows the 'Advanced Configuration' window for a captive portal instance named 'TestCP1'. The 'Verification' dropdown is set to 'Local'. The 'Admin mode' is set to 'Enable'. The 'Protocol' is set to 'http'. The 'User group name' is set to 'Default'. The 'Redirect' is set to 'Disable'. The 'Redirect URL' is empty. The 'Away time' is set to 60 minutes. The 'Session timeout' is set to 0 minutes. The 'Max bandwidth upstream' and 'Max bandwidth downstream' are both set to 0 Mbps. The 'Locale count' is set to 0. The 'Delete instance' checkbox is unchecked. The 'Save' and 'Cancel' buttons are at the bottom right.

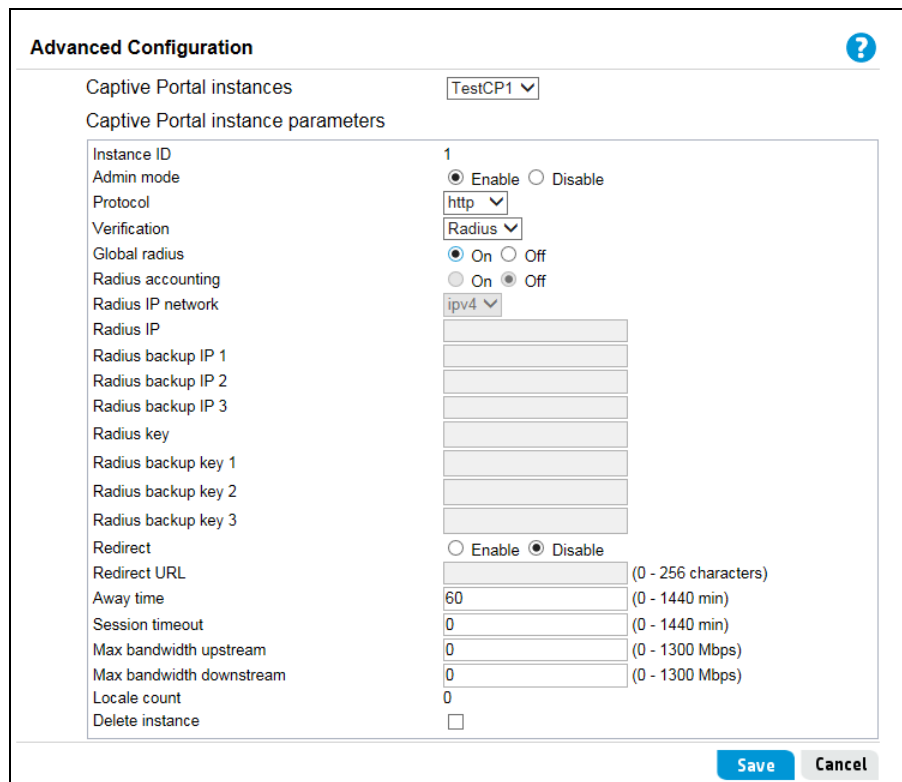
Advanced Configuration	
Captive Portal instances	TestCP1
Captive Portal instance parameters	
Instance ID	1
Admin mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Protocol	http
Verification	Local
User group name	Default
Redirect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Redirect URL	(0 - 256 characters)
Away time	60 (0 - 1440 min)
Session timeout	0 (0 - 1440 min)
Max bandwidth upstream	0 (0 - 1300 Mbps)
Max bandwidth downstream	0 (0 - 1300 Mbps)
Locale count	0
Delete instance	<input type="checkbox"/>

User group name

The user group associated with this instance. Each captive portal user is associated with a group, and a group is associated with a captive portal instance. See ["Local user/group association"](#) on page 106.

RADIUS verification

The additional following fields are displayed on the Advanced Configuration page when **Verification** is set to **Radius**.



The screenshot shows the 'Advanced Configuration' window for a captive portal instance named 'TestCP1'. The 'Verification' dropdown is set to 'Radius'. The 'Admin mode' is set to 'Enable'. The 'Protocol' is set to 'http'. The 'Global radius' is set to 'On'. The 'Radius accounting' is set to 'Off'. The 'Radius IP network' is set to 'ipv4'. The 'Radius IP' is empty. The 'Radius backup IP 1', 'Radius backup IP 2', and 'Radius backup IP 3' are all empty. The 'Radius key', 'Radius backup key 1', 'Radius backup key 2', and 'Radius backup key 3' are all empty. The 'Redirect' is set to 'Disable'. The 'Redirect URL' is empty. The 'Away time' is set to 60 minutes. The 'Session timeout' is set to 0 minutes. The 'Max bandwidth upstream' and 'Max bandwidth downstream' are both set to 0 Mbps. The 'Locale count' is set to 0. The 'Delete instance' checkbox is unchecked. The 'Save' and 'Cancel' buttons are at the bottom right.

Advanced Configuration	
Captive Portal instances	TestCP1
Captive Portal instance parameters	
Instance ID	1
Admin mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Protocol	http
Verification	Radius
Global radius	<input checked="" type="radio"/> On <input type="radio"/> Off
Radius accounting	<input type="radio"/> On <input checked="" type="radio"/> Off
Radius IP network	ipv4
Radius IP	
Radius backup IP 1	
Radius backup IP 2	
Radius backup IP 3	
Radius key	
Radius backup key 1	
Radius backup key 2	
Radius backup key 3	
Redirect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Redirect URL	(0 - 256 characters)
Away time	60 (0 - 1440 min)
Session timeout	0 (0 - 1440 min)
Max bandwidth upstream	0 (0 - 1300 Mbps)
Max bandwidth downstream	0 (0 - 1300 Mbps)
Locale count	0
Delete instance	<input type="checkbox"/>

Global radius

When Verification is set to **Radius**, you can select **On** to use the **Global RADIUS** server list for authenticating captive portal clients (see “[Configuring global RADIUS servers](#)” on page 29). If set to **Off**, the RADIUS servers must be configured on this page.

Radius accounting

To track the resources that captive portal clients use, such as the network connection time and amount of data transmitted or received, you can enable the RADIUS accounting feature. When enabled, RADIUS accounting functions on all local or globally configured servers.

Radius IP network

Specify whether the local RADIUS server IP addresses are IPv4 or IPv6 addresses.

Radius IP

The IPv4 or IPv6 address of the primary RADIUS server for this wireless community. The AP first attempts to authenticate clients using the primary server, if this server fails the backup servers are then tried.

Radius backup IP 1-3

Up to three IPv4 or IPv6 backup RADIUS server addresses. After an authentication failure using the primary server, the backup servers are then tried in sequence.

Radius key

The primary RADIUS server shared secret key. Specify up to 63 alphanumeric and special characters that are case sensitive. The key must match the key configured on the primary RADIUS server.

Radius backup key 1-3

The RADIUS shared secret keys for backup server IPs 1-3. Each key must match the key configured on the same numbered backup RADIUS server.

Community binding

The Community Binding page associates a captive portal instance to a virtual service community (VSC). All users that attempt to authenticate on the community have the captive portal instance settings applied.

To configure captive portal community binding, select **Captive Portal > Community Binding**. The Community Binding page displays.

Community Binding	
Radio	1
vsc	
0	TestCP1
1	TestCP1
2	
3	
4	
5	
6	
7	
<div>Save Cancel</div>	

The following describes the fields on the captive portal Community Binding page.

Radio

The radio associated with the wireless communities (VSCs) that are to be configured.

VSC

The list of VSC IDs. A captive portal instance can be associated with multiple VSCs.

Instance name

From the list, select the instance to associate with each VSC. If the list is blank, no instance is associated with the VSC.

Web customization

When users initiate access to a wireless community that is associated with a captive portal instance, an authentication page displays. The captive portal authentication page can be customized by changing text, color, and images to create a locale. Up to three locales can be created and associated with a captive portal instance, which enables the display of captive portal authentication pages in multiple languages (up to three). The language of choice can then be selected from the upper left-hand side of the main captive portal page.

Creating a web locale

The AP has no web locale pages configured by default. To create a web locale, first assign a name to the locale, and then click **Save**.

To configure a captive portal web locale, select **Captive Portal > Web Customization**. The Web Customization page displays.

In the **Web customization** section of the page, select **Create** for **Captive Portal web locale** and enter a name of 1-32 characters in the **Web locale name** box. Click **Save** to create the locale. The **Captive Portal web locale parameters** are then displayed and can be configured.

The screenshot shows the 'Web Customization' page. It has a title bar with a question mark icon. The page is divided into three main sections: 'Web binary upload', 'Web customization', and 'Web preview'. The 'Web binary upload' section has two rows: 'Upload web customization image' with a text input and a 'Browse...' button, and 'Delete web customization image' with a dropdown menu. Both rows have 'Upload' and 'Delete' buttons. The 'Web customization' section has a 'Captive Portal web locale' dropdown set to 'Create'. Below it is the 'Captive Portal web locale parameters' section, which contains a 'Web locale name' text input (with a '(1 - 32 characters)' hint) and a 'Captive Portal instances' dropdown set to 'TestCP1'. 'Save' and 'Cancel' buttons are at the bottom right of this section. The 'Web preview' section has a 'Captive Portal web locale' dropdown and a 'Captive Portal web locale parameters preview' label.

The following parameters are on the Web Customization page.

Upload web customization image

Click **Browse** to locate an image file on the management computer that can be used on the captive portal web page. Click **Upload** to store the image file on the AP.

Delete web customization image

Select a stored image file in the list and then click **Delete** to remove it from the AP.

Captive portal web locale

To create a new web locale, select **Create** from the available list. To view or update an existing web locale, select its name from the list. After a web locale has been created or selected, the **Captive portal web locale parameters** are displayed.

Web locale name

This field is displayed only if **Create** is selected from the **Captive Portal web locale** list. Enter a name to assign to the page. The name can be from 1 to 32 alphanumeric characters.

Captive Portal instances

This field is displayed only when **Create** is selected from the **Captive Portal web locale** list. From the list, select the captive portal instance to which this locale is associated.

Multiple locales can be associated with a captive portal instance. When a wireless community associated with a captive portal instance is accessed by a user, links for all the locales are displayed on the authentication page. The user then selects the link for the appropriate locale.

Customizing a web locale

After a captive portal web locale has been created, the web page customization parameters can be configured. The following describes the parameters on the Web Customization page.

Web customization

Captive Portal web locale Locale1 ▾

Captive Portal web locale parameters

Locale ID	1
Instance ID	1
Instance name	TestCP1
Background image name	HPBackground.gif ▾
Logo image name	HPLogo.gif ▾
Foreground color	#FFFFFF
Background color	#E5E8E8
Separator	#E5E8E8
Locale label	English
Locale	en
Account image	HPLogin.gif ▾
Account label	Enter your Username
User label	Username:
Password label	Password:
Button label	Connect
Fonts	'MS UI Gothic', arial, sans-serif ▴ ▾
Browser title	Captive Portal ▴ ▾
Browser content	Welcome to the Wireless Network ▴ ▾
Content	To start using this service, enter your credentials ▴ ▾
Acceptance use policy	Acceptance Use Policy. ▴ ▾
Accept label	Check here to indicate that you have read and agree to the ▴ ▾
No accept text	Error: You must acknowledge the Acceptance Use Policy. ▴ ▾
Work in progress text	Connecting, please be patient... ▴ ▾
Denied text	Error: Invalid Credentials, please try again. ▴ ▾
Welcome title	Congratulations! ▴ ▾
Welcome content	You are now authorized and connected ▴ ▾
Delete locale	<input type="checkbox"/>

Save Cancel

Locale ID

The ID that is automatically assigned to the locale when it is created. The ID cannot be configured.

Instance ID

The ID of the captive portal instance associated with the locale.

Instance name

The user-configured name of the captive portal instance.

Background image name

The name of the image file that displays as the page background. Click **Upload web customization image** to upload images to the AP for use with captive portal instances.

Logo image name

The name of the image file that displays in the top left corner of the page. This image is typically a company logo. First upload your logo image to the AP, and then select it from the list.

Foreground color

The authentication page foreground color in a 6-digit hexadecimal format (the field accepts 1 to 32 characters). The default value is #FFFFFF.

Background color

The authentication page background color in a 6-digit hexadecimal format (the field accepts 1 to 32 characters). The default value is #E5E8E8.

Separator

The 6-digit hexadecimal code for the color of the thick horizontal line between the page header and the page body. The field accepts 1 to 32 characters, and the default value is #E5E8E8.

Locale label

A text description of 1 to 32 characters that identifies the locale. The default is English.

Locale

An abbreviation for the locale. Range 1 to 32 characters. The default is en.

Account image

The file name of the image indicating an authenticated login that displays above the login field.

Account label

The displayed text that tells a user to enter a user name. The range is from 0 to 32 characters.

User label

A text description of 0 to 32 characters that identifies the user name field.

Password label

A text description of 0 to 64 characters that identifies the user password field.

Button label

The text label for the page button that must be clicked to submit a user name and password for authentication. The range is from 2 to 32 characters. The default is Connect.

Fonts

The name of the font to use for all text on the authentication page. Multiple font names, separated by commas, can be listed. When the first font is not available on a client system, the next available font in the list is used. Font names that include spaces must be enclosed in quotes. You can enter 1 to 512 characters. The default font list is "MS UI Gothic", arial, sans-serif.

Browser title

The text that displays in the browser title bar. Enter 1 to 128 characters. The default text is Captive Portal.

Browser content

The text that displays next to the logo in the page header. Enter 1 to 128 characters. The default is Welcome to the Wireless Network.

Content

The text that displays below the user name and password fields. Enter 0 to 256 characters. The default text is To start using this service, enter your credentials and click the connect button.

Acceptance use policy

The text that is displayed in the Acceptance Use Policy box. Enter 0 to 8192 characters. The default text is Acceptance Use Policy.

Accept label

The text that instructs users to accept the Acceptance Use Policy by selecting the check box. Enter 0 to 128 characters. The default text is Check here to indicate that you have read and accepted the Acceptance Use Policy.

No accept text

The text that is displayed in a pop-up window when a user tries to login without first selecting the Acceptance Use Policy check box. Enter 1 to 128 characters. The default text is: Error: You must acknowledge the Acceptance Use Policy before connecting!

Work in progress text

The text that is displayed during authentication. Enter 1 to 128 characters. The default text is: Connecting, please be patient....

Denied text

The text that is displayed when a user fails authentication. Enter 1 to 128 characters. The default text is: Error: Invalid Credentials, please try again!

Welcome title

The text that is displayed when a user has successfully authenticated to a wireless community. Enter 1 to 128 characters. The default text is: Congratulations!

Welcome content

The text that is displayed when a user is successfully connected to the network. Enter 0 to 256 characters. The default text is: You are now authorized and connected to the network.

Delete locale

To delete the current locale, select this option and click Save.

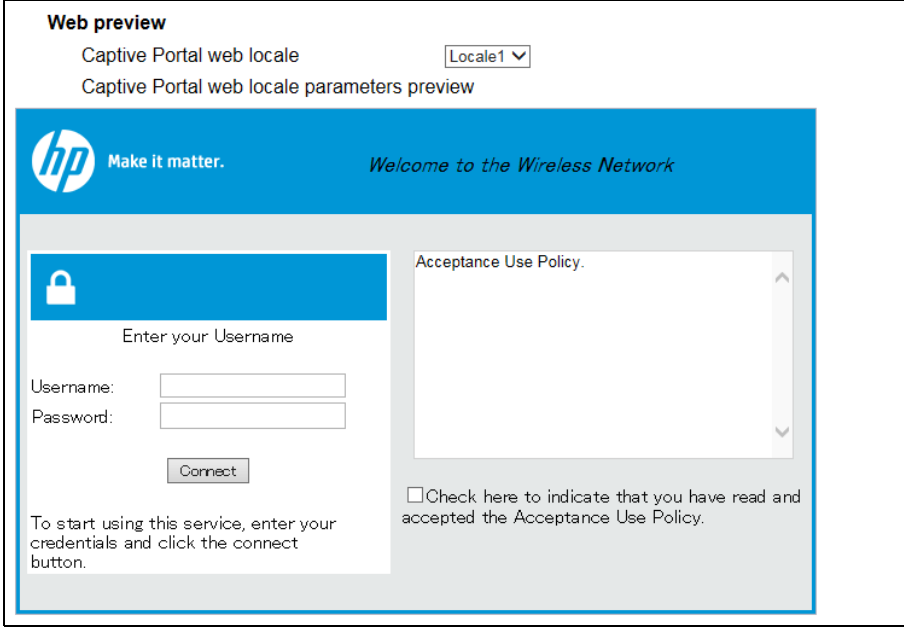
Web preview

To display a preview of the authentication page, select the locale name from the Captive Portal Web Locale list.

Previewing a web locale

After a web locale customization parameters are configured, you can view the locale web page in the **Web preview** section of the Web Customization page.

Select the locale name from the Captive Portal web locale list. The locale web page displays.



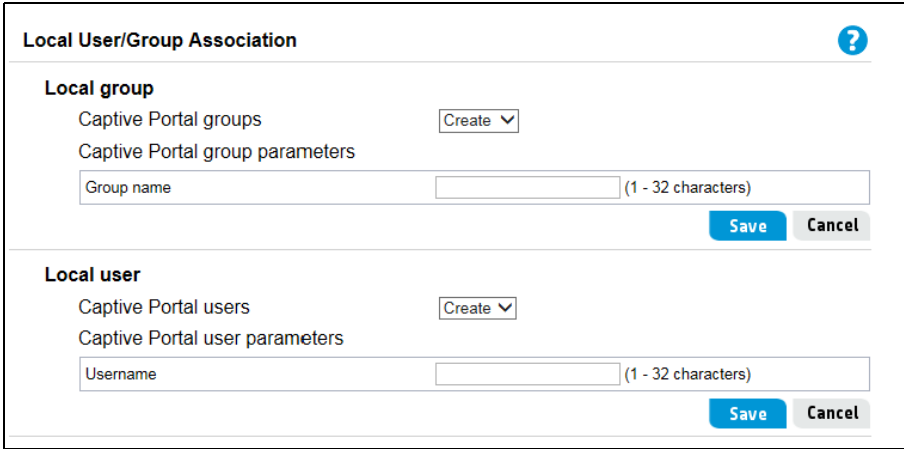
The screenshot shows the 'Web preview' section of a configuration interface. At the top, there's a dropdown menu for 'Captive Portal web locale' set to 'Locale1'. Below it, the text 'Captive Portal web locale parameters preview' is displayed. The main preview area shows a login page with the HP logo and the slogan 'Make it matter.' The page title is 'Welcome to the Wireless Network'. The login form includes a 'Username' field, a 'Password' field, and a 'Connect' button. To the right of the login form is an 'Acceptance Use Policy' section with a checkbox for 'Check here to indicate that you have read and accepted the Acceptance Use Policy.' Below the login form, there is a note: 'To start using this service, enter your credentials and click the connect button.'

Local user/group association

A captive portal instance can be configured for both guest users and authorized users. Guest users do not have assigned user names and passwords. Authorized users must first submit a valid user name and password to be validated against a local database or RADIUS server. Typically, authorized users are assigned to a different captive portal instance and wireless community than guest users.

Use the Local User/Group Association page to configure up to 128 authorized users in the local database.

To configure captive portal local users and groups, select **Captive Portal > Local User/Group Association**. The Local User/Group Association page displays.



The screenshot shows the 'Local User/Group Association' configuration page. It has two main sections: 'Local group' and 'Local user'. Each section has a 'Create' dropdown menu. Below the 'Local group' section, there is a 'Group name' field with a character limit of '(1 - 32 characters)' and 'Save' and 'Cancel' buttons. Below the 'Local user' section, there is a 'Username' field with a character limit of '(1 - 32 characters)' and 'Save' and 'Cancel' buttons.

Creating local captive portal groups

In the **Local group** section of the page, select **Create** for **Captive Portal groups** and enter a name of 1-32 characters in the **Group name** box. Click **Save** to create the group. The **Captive Portal web locale parameters** are then displayed and can be configured.

The following parameters on the Local User/Group Association page are used to create a captive portal local group.

Captive Portal groups

To create a new group, select **Create**. After you create a group or select an existing group from the **Captive Portal Groups** list, additional parameters display on the page.

Group name

Specify a name for the new local group.

Delete group

To delete the current group, select this option and click **Save**.

Creating local captive portal users

In the **Local user** section of the page, select **Create** for **Captive Portal users** and enter a name of 1-32 characters in the **Username** box. Click **Save** to create the user. The **Captive Portal user parameters** are then displayed and can be configured.

The following parameters on the Local User/Group Association page are used to create a captive portal local user.

Captive Portal users

To create a new user, select **Create**. To configure settings for a user, select the name from the list.

Username

Specify a name for the local user. Enter 1-32 characters for the name.

After you create a user or select an existing user from the **Captive Portal Users** menu, additional fields display on the page.

The screenshot shows a web form titled "Local user". At the top, there is a section "Captive Portal users" with a dropdown menu showing "John". Below this is a section "Captive Portal user parameters". This section contains several input fields: "User password" (with a note "(8 - 64 characters)"), "Away time" (with a note "(0 - 1440 minutes)"), "Group name" (with a dropdown menu showing "Default" and "Group1"), "Max bandwidth upstream" (with a note "(0 - 1300 Mbps)"), "Max bandwidth downstream" (with a note "(0 - 1300 Mbps)"), and a "Delete user" checkbox. At the bottom right of the form are "Save" and "Cancel" buttons.

The following parameters on the Local User/Group Association page are used to configure settings for a captive portal local user.

Captive Portal users

Select the name of the user for which you want to configure settings.

User password

Enter 8 to 64 alphanumeric and special characters for the user's password. The user must enter this password to log into the captive portal and gain access to the network.

Away time

The time that a client entry is retained in the captive portal authenticated client list after it has disassociated from the AP. Specify a time between 0 and 1440 minutes. The default setting is 0 minutes.

Note

Each captive portal instance also has a configured **Away time** setting. See [“Advanced configuration” on page 96](#). The local user timeout value has precedence over the value configured for the captive portal instance.

Group name

Select the group to which the user belongs. Each captive portal instance supports a particular user group.

Note

Each Group must contain at least one user in order to avoid captive portal authentication failures.

Maximum bandwidth upstream

The maximum speed at which a client can send data to the network when using the captive portal. Specify a value between 0 and 1300 Mbps. The default value is 0, which means that no limit is enforced.

Maximum bandwidth downstream

The maximum speed at which a client can receive data from the network when using the captive portal. Specify a value between 0 and 1300 Mbps. The default value is 0, which means that no limit is enforced.

Delete user

To delete the current user, select this option and click **Save**.

Client list

The Client List page displays information about clients that have authenticated or failed authentication on the configured captive portal instances.

To view the captive portal client list, select **Captive Portal > Client List**. The Client List page displays.

Client List ?

Authenticated clients

Total number of authenticated clients 0

MAC address	IP address	Username	Protocol mode	Verify mode	VSC ID	Radio ID	Captive Portal ID	Session timeout	Away timeout	Rx packets	Tx packets	Rx bytes	Tx bytes
-------------	------------	----------	---------------	-------------	--------	----------	-------------------	-----------------	--------------	------------	------------	----------	----------

Failed authentication clients

Total number of failed authentication clients 0

MAC address	IP address	Username	Verify mode	VSC ID	Radio ID	Captive Portal ID	Failure time
-------------	------------	----------	-------------	--------	----------	-------------------	--------------

Refresh

The following parameters are on the Client List page.

Total number of authenticated clients

The number of clients that have successfully authenticated on any captive portal instance. This number includes only clients that are currently authenticated.

Total number of failed authentication clients

The number of clients that have failed authentication on any captive portal instance.

MAC address

The MAC address of the client.

IP address

The IPv4 or IPv6 address of the client. If the client has a valid IPv4 address assigned, it will be displayed here. Otherwise, a global IPv6 address, either from DHCPv6, Autoconfiguration, or statically configured, will be used.

Username

The client's captive portal user name.

Protocol mode

The connection protocol used by the client (HTTP or HTTPS).

Verify mode

The authentication method used for the captive portal client; either Guest, Local, or RADIUS.

VSC ID

The virtual service community (VSC) to which the user is associated.

Radio ID

The ID of the radio. Radio 1 for 2.4 GHz band, or Radio 2 for 5 GHz band.

Captive Portal ID

The captive portal instance ID to which the client is associated.

Session timeout

The remaining time (in seconds) of the valid captive portal session, after which the client is deauthenticated.

Away timeout

The remaining time (in seconds) for a dissociated valid client before it is deauthenticated.

Rx packets

The number of received IP packets from the client station.

Tx packets

The number of IP packets transmitted to the client station.

Rx bytes

The number of bytes received from the client station.

Tx bytes

The number of bytes transmitted to the client station.

Failure time

The timestamp for when the client station failed authentication. (**Failed authentication clients** list only.)

Example of guest captive portal configuration

This example shows you how to create a captive portal on the M330 for unauthorized guest access to a wireless network.

Initial settings

Starting with a factory default M330, first configure **Basic wireless network** as the Network Environment, and then proceed to configure the basic radio settings in the Quick Setup wizard.

Step 3: Specify wireless network settings

Radio	1
Wireless mode	IEEE 802.11b/g/n
Identify the wireless network	
Network name (SSID)	Guest
Secure the wireless network	
Security method	Disabled

Save **Cancel**

Select the **Radio** and **Wireless mode** for the captive portal. Typically, **Radio 1** in the **IEEE 802.11b/g/n** mode provides the widest support for guest users.

Set the Network name (SSID) for the captive portal, for example, **Guest**.

Set the **Security method** to **Disabled** to allow guest users unauthenticated access to the network.

Basic configuration

Select **Captive Portal > Basic Configuration** and set the **Captive portal mode** to **Enable**. Click **Save**.

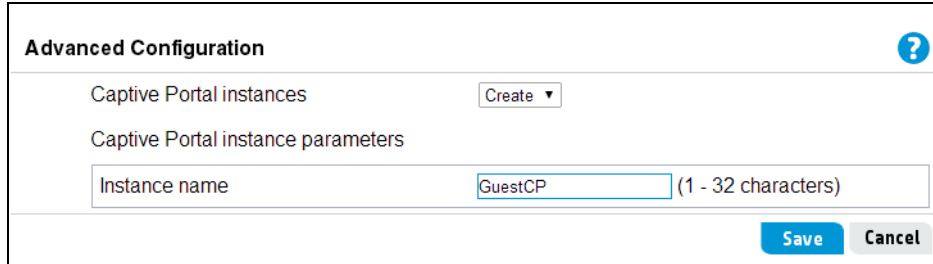
Basic Configuration ?

Captive Portal mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Authentication timeout	300 (60 - 600 seconds)
Additional HTTP port	0 (1025 - 65535, 0 disables)
Additional HTTPS port	0 (1025 - 65535, 0 disables)
Instance count	0
Group count	1
User count	0

Save **Cancel**

Advanced configuration

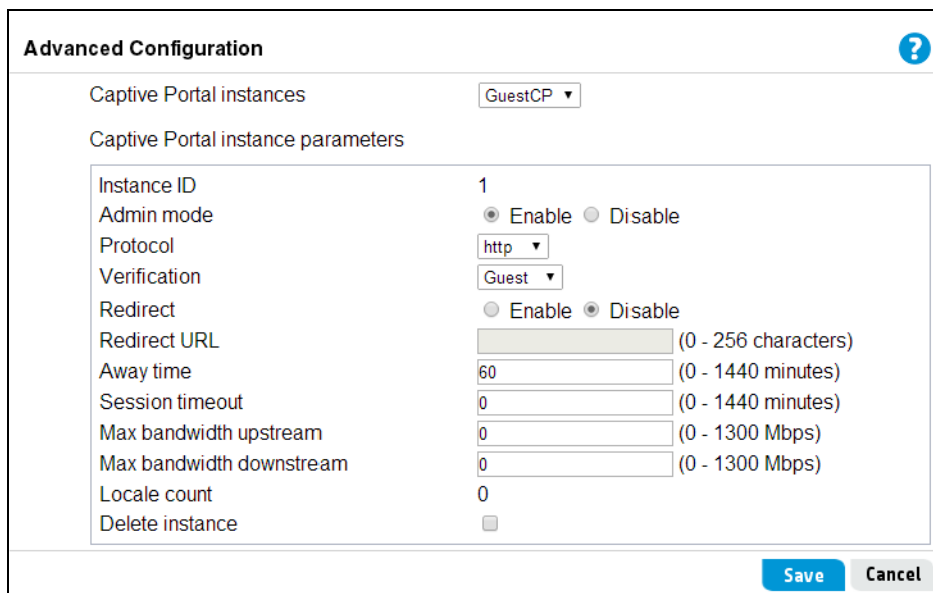
Select **Captive Portal** > **Advanced Configuration** and create a captive portal instance.



The dialog box is titled "Advanced Configuration" with a help icon. It contains two sections: "Captive Portal instances" with a "Create" button, and "Captive Portal instance parameters" with an "Instance name" field containing "GuestCP" and a "(1 - 32 characters)" label. At the bottom are "Save" and "Cancel" buttons.

Set **Captive portal instances** to **Create**, and then enter an **Instance name**, for example, **GuestCP**. Click **Save**. The captive portal instance settings are displayed.

Note that **Verification** is set to **Guest** by default, so there is no need to change any settings. If you do changes any other settings, click **Save** again.



The dialog box shows the "GuestCP" instance selected. The "Captive Portal instance parameters" section is expanded, displaying the following settings: Instance ID (1), Admin mode (radio buttons for Enable and Disable, with Enable selected), Protocol (http), Verification (Guest), Redirect (radio buttons for Enable and Disable, with Disable selected), Redirect URL (empty field, 0 - 256 characters), Away time (60, 0 - 1440 minutes), Session timeout (0, 0 - 1440 minutes), Max bandwidth upstream (0, 0 - 1300 Mbps), Max bandwidth downstream (0, 0 - 1300 Mbps), Locale count (0), and a Delete instance checkbox. "Save" and "Cancel" buttons are at the bottom.

Community binding

Select **Captive Portal** > **Community Binding**.

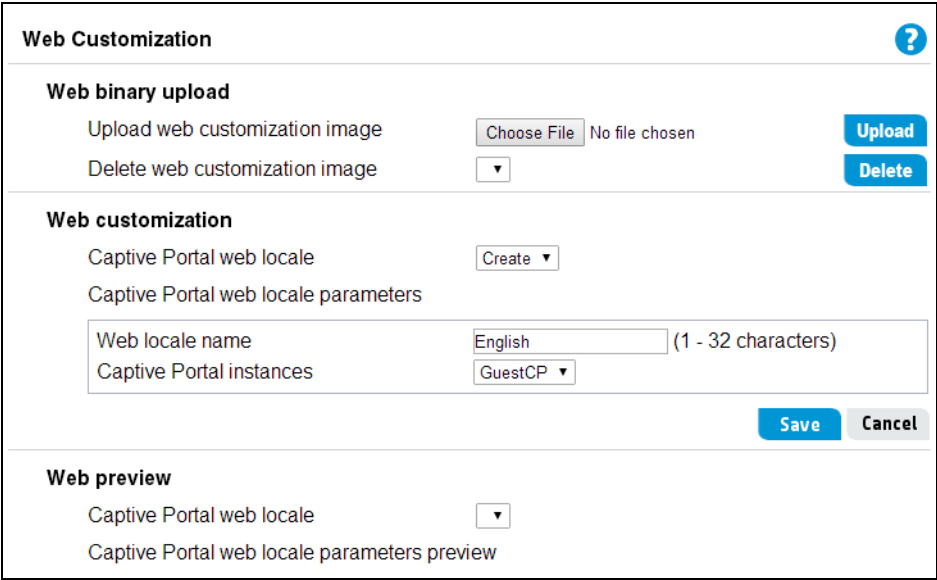
For **Radio 1**, **VSC 0**, select the captive portal instance **GuestCP** from the list. Click **Save**.



The **Community Binding** window features a title bar with a question mark icon. It contains a **Radio** dropdown menu set to **1**. Below this is a **VSC** section with a list of indices from 0 to 7. Each index has a corresponding dropdown menu; the dropdown for index 0 is currently set to **GuestCP**, while the others are empty. At the bottom right, there are **Save** and **Cancel** buttons.

Web customization

Select **Captive Portal** > **Web Customization** and create a captive portal web locale.



The **Web Customization** window has a title bar with a question mark icon. It is divided into three main sections. The **Web binary upload** section includes an **Upload web customization image** button with a **Choose File** dialog showing **No file chosen**, and a **Delete web customization image** dropdown menu. The **Web customization** section contains a **Captive Portal web locale** dropdown set to **Create**, followed by **Captive Portal web locale parameters** which include a **Web locale name** text field (containing **English** with a **(1 - 32 characters)** hint) and a **Captive Portal instances** dropdown set to **GuestCP**. The **Web preview** section at the bottom has a **Captive Portal web locale** dropdown and a **Captive Portal web locale parameters preview** area. **Save** and **Cancel** buttons are located at the bottom right of the window.

Set **Captive Portal web locale** to **Create** and enter a **Web locale name**, for example, **English**. Click **Save**. The captive portal web locale customization settings are displayed.

Web Customization

Web binary upload

Upload web customization image

Choose File

No file chosen

Delete web customization image

▼

Upload

Delete

Web customization

Captive Portal web locale

English ▼

Captive Portal web locale parameters

Locale ID	1
Instance ID	1
Instance name	GuestCP
Background image name	HPBackground.gif ▼
Logo image name	HPLogo.gif ▼
Foreground color	#FFFFFF
Background color	#E5E8E8
Separator	#E5E8E8
Locale label	English
Locale	en
Account image	HPLogin.gif ▼
Account label	Enter your Username

Configure the web customization settings for the captive portal web locale. For details on these settings, see [“Customizing a web locale” on page 102](#). Click **Save**.

Under **Web preview** at the bottom of the Web Customization page, select **English** from the list for **Captive Portal web locale** to view the customized web page.

Web preview

Captive Portal web locale

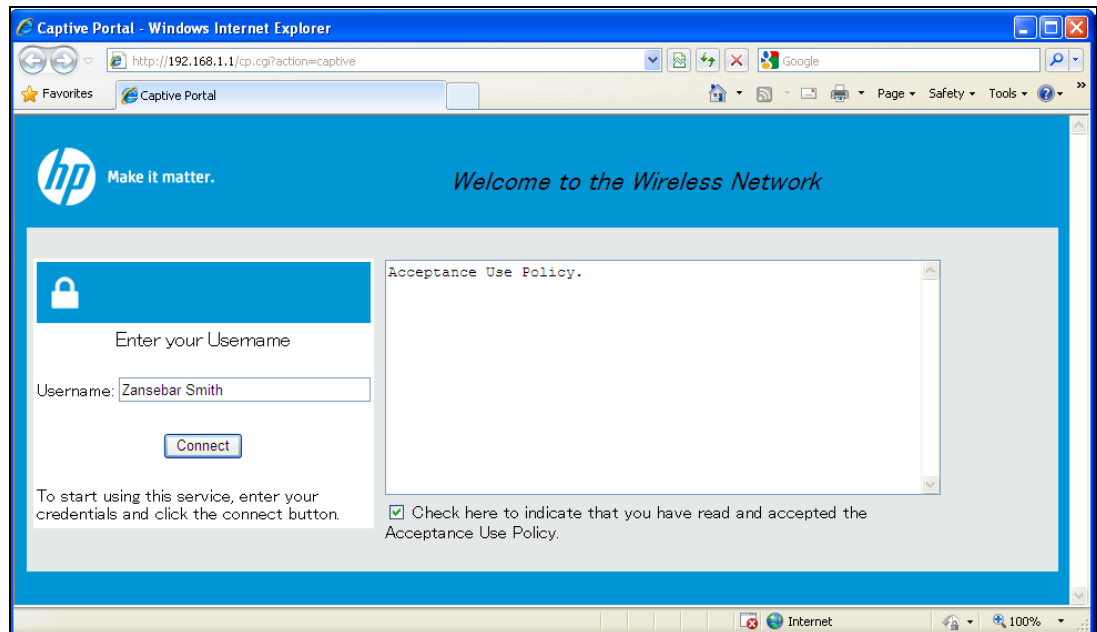
English ▼

Captive Portal web locale parameters preview

Example of guest captive portal configuration 113

Test captive portal client access

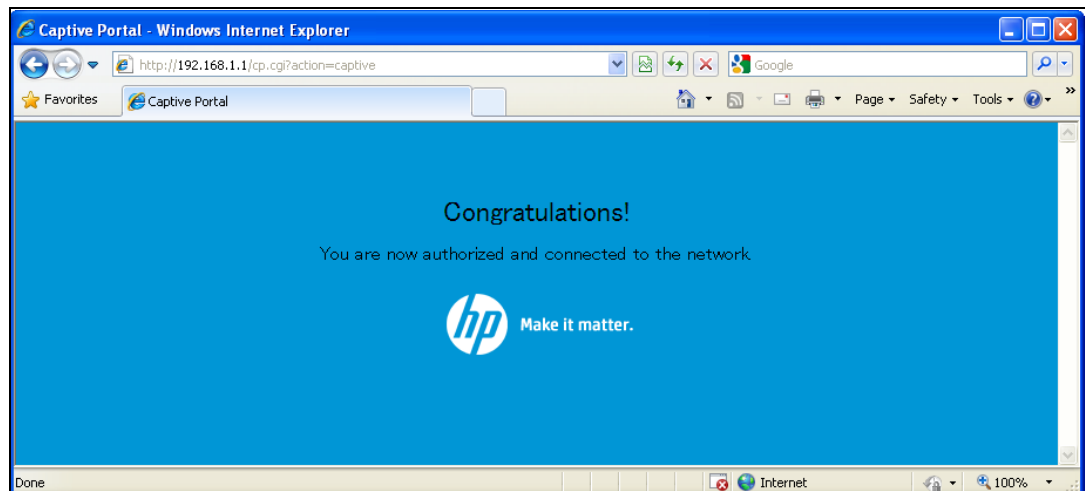
From any wireless client, such as a notebook computer, locate the **Guest** SSID network and connect.



Either immediately (on some smartphones) or when you launch a web browser, the captive portal authentication page displays. Enter a **Username** and check the **Acceptance Use Policy** to log in to the network. The captive portal welcome page displays. You now have access to the network and should be able to browse the Internet.

Note

With the Guest captive portal instance used in this example, **Username** is solely for information purposes. No user authentication is performed. The user can choose to leave **Username** blank.



On the M330, select **Captive Portal** > **Client List** to view wireless clients logged in to the captive portal network.

Client List

?

Authenticated clients

Total number of authenticated clients3

MAC address	IP address	Username	Protocol mode	Verify mode	VSC ID	Radio ID	Captive Portal ID	Session timeout	Away timeout	Rx packets	Tx packets	Rx bytes	Tx bytes
80:be:05:34:5e:d9	15.226.15.52	Mandrake Curvey	http	guest	0	1	1	0	3004 s	383	171	32330	75907
98:fe:94:21:69:ef	15.226.15.60	Bombast Blevy	http	guest	0	1	1	0	0	126	23	10241	2949
7c:c5:37:24:ac:ca	15.226.15.55	Zansebar Smith	http	guest	0	1	1	0	0	4919	5670	771943	6282254

Failed authentication clients

Total number of failed authentication clients0

MAC address	IP address	Username	Verify mode	VSC ID	Radio ID	Captive Portal ID	Failure time

Refresh

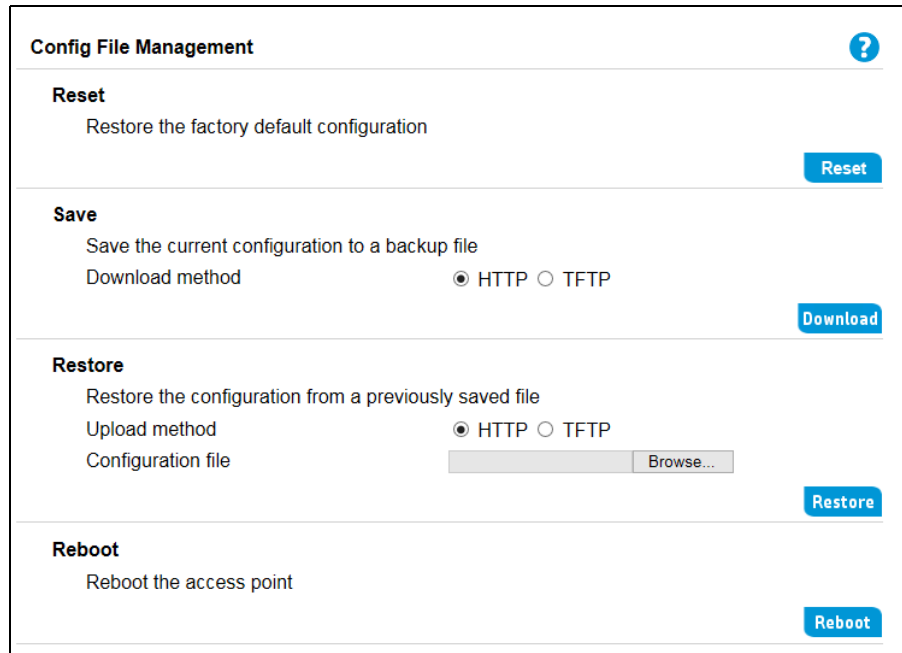
The name entered by the captive portal client is shown in the **Username** column.

When a captive portal client does not enter a username in this unauthenticated example, the name “guest” appears in the **Username** column.

10 Maintenance

Configuration file management

The configuration file contains all the settings that customize the operation of the M330. You can save and restore the configuration file by selecting **Maintenance > Config File Management**.



The screenshot shows the 'Config File Management' web interface. It has a title bar with a question mark icon. Below the title bar, there are four main sections: 'Reset', 'Save', 'Restore', and 'Reboot'. Each section has a description of the action and a corresponding button. The 'Reset' section has a 'Reset' button. The 'Save' section has a 'Download' button and a radio button for 'HTTP' (selected) and 'TFTP'. The 'Restore' section has a 'Restore' button and a radio button for 'HTTP' (selected) and 'TFTP'. The 'Reboot' section has a 'Reboot' button. The 'Restore' section also has a 'Configuration file' field with a 'Browse...' button.

Config File Management	
Reset Restore the factory default configuration	Reset
Save Save the current configuration to a backup file Download method: <input checked="" type="radio"/> HTTP <input type="radio"/> TFTP	Download
Restore Restore the configuration from a previously saved file Upload method: <input checked="" type="radio"/> HTTP <input type="radio"/> TFTP Configuration file: <input type="text"/> Browse...	Restore
Reboot Reboot the access point	Reboot

Reset

See “Resetting to factory defaults” on page 137.

Save

The Save feature enables you to back up your configuration settings so that they can be easily restored in case of failure.

Before you install new software, you should always back up your current configuration.

To start the process, select a **Download method** and then click **Download**.

For HTTP downloads, you are prompted for the location in which to save the configuration file, namely **config.xml**. For TFTP downloads, specify the file path and file name under which to save the file, and the TFTP server name. The name of the configuration file can have up to 255 characters, including the .xml file name extension and the path to the directory where you want to save the file. File names should not contain spaces or the these characters < > | \ : () & ; # ? * % ` ' " / .

Restore

The Restore feature enables you to load a previously saved configuration file.

For an HTTP restore, click **Browse** to select to the configuration file that you want to restore, then click **Restore**.

For a TFTP restore, specify the file path and file name on the TFTP server, and enter the TFTP server address. Then, click **Restore**. The name of the configuration file can have up to 255 characters, including the .xml file name extension and the path to the directory where the file is saved. File names should not contain spaces or the these characters < > | \ : () & ; # ? * % ` ' " / .

After restoring the configuration file, the system automatically reboots.

Note

The M330 automatically restarts when the upload is completed.

Reboot

For maintenance purposes or as a troubleshooting measure, you can reboot the M330 by clicking **Reboot**.

The process may take several minutes during which time the AP will be unavailable. The M330 resumes normal operation with the same configuration settings it had before the reboot.

Software updates

To update the M330 software, select **Maintenance > Manage Software**. The Manage Software page displays.

The Manage Software page shows the AP model information, as well as the current active (primary) image and backup (secondary) image versions. This page also enables a new software image file to be uploaded to the AP using HTTP or TFTP protocols.

Manage Software

Software information

Model	HP M330 802.11ac Access Point
Primary image	V1.0.0.0-M330-B000-1
Secondary image	V0.0.0.39-M330-B000-0

Switch

Software upgrade

Upload method

☒ HTTP ☐ TFTP

New firmware image

Browse...

Upgrade

Software information

The M330 maintains both a primary software image and a backup image. The M330 always tries to boot with the primary image. If it fails to load, then the secondary image is used. Whenever such a failover occurs, the system creates a log message to help you troubleshoot the software failure.

Switching the software image

The **Software information** area shows the active image and backup image versions. To make the backup image the active image, and the active image the backup image, click **Switch**.

The AP reboots using the new image. The process may take several minutes during which time the AP will be unavailable. Do not power down the AP while the image switch is in progress. When the image switch is complete, the AP restarts. The M330 resumes normal operation with the same configuration settings it had before the image switch.

Software upgrade

When a software upgrade is available, you can download the image to the M330.

Caution

- Before updating be sure to check for update issues in the Release Notes.
- Even though configuration settings are preserved during software updates, HP recommends that you back up your configuration settings before updating. See [“Configuration file management” on page 117](#).

To update the M330 software using HTTP, click **Browse** to locate the software file (with the extension *.img*) and then click **Upgrade**.

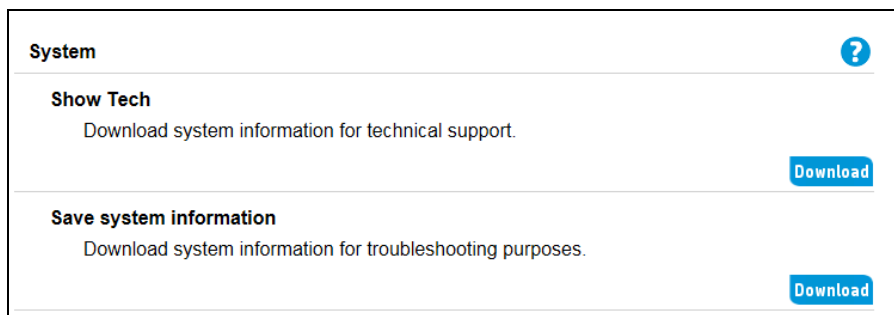
To update the software using TFTP, specify the file path and file name on the TFTP server, and enter the TFTP server address. Then, click **Upgrade**.

At the end of the update process, the M330 automatically restarts, disconnecting the current management session. Once the M330 resumes operation, you can reconnect.

System information

The System page enables you to download logs, settings, system tools outputs, and other information that customer support may find helpful in diagnosing problems.

To download system information, select **Maintenance > System**.



The screenshot shows a web interface for the 'System' page. At the top, there is a header 'System' with a question mark icon. Below this, there are two main sections. The first section is titled 'Show Tech' and contains the text 'Download system information for technical support.' followed by a blue 'Download' button. The second section is titled 'Save system information' and contains the text 'Download system information for troubleshooting purposes.' followed by another blue 'Download' button.

In the **Show tech** area, you can download a file that can be read in a text editor. The file contains configuration settings, including those that have been customized by the user. The file is named **showtech.rtf** by default.

In the **Save system information** area, you can download an encrypted binary file. Although you cannot read this file, you can provide it to customer support to assist in debugging efforts. This file contains additional configuration and device information. It is named **showdev.out** by default.

When you click **Download** in either section, you are prompted to select a location to save the file.

Viewing the EULA

This page displays the HP End User License Agreement content, and other third-party licenses and copyright notices.

To view the notices and license information, select **Maintenance > EULA**.

HP End User License Agreement

HP End User License Agreement

End User License Agreement
=====

PLEASE READ CAREFULLY BEFORE USING THIS EQUIPMENT: This End-User license Agreement ("EULA") is a legal agreement between (a) you (either an individual or a single entity) and (b) Hewlett-Packard Company or in-country legal entity ("HP") that governs your use of any Software Product, which is either (i) installed on or made available by HP for use with your HP product ("HP Product") or (ii) made available as part of the HP product portfolio for use on a standalone basis ("HP Software Product"), that is not otherwise subject to a separate license agreement between you and HP or its suppliers. Other software may contain a EULA in its online documentation. The term "Software Product" means computer software and may include associated media, printed materials and "online" or electronic documentation. An amendment or addendum to this EULA may accompany the HP Product or HP Software Product.

RIGHTS IN THE SOFTWARE PRODUCT ARE OFFERED ONLY ON THE CONDITION THAT YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS EULA. BY INSTALLING, COPYING, DOWNLOADING OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOUR SOLE REMEDY IS TO RETURN THE ENTIRE UNUSED PRODUCT (HARDWARE AND SOFTWARE) WITHIN 14 DAYS FOR A REFUND, SUBJECT TO THE REFUND POLICY OF YOUR PLACE OF PURCHASE.

The HP End User License Agreement has already been accepted on this device

Third party licenses and copyright notices

☐ GPL Version 2 License

[Click here to learn how to get GPLv2 sources](#)

☐ Other Copyrights and Licenses

11 Tools

System log

The system log is a comprehensive list of system messages and kernel messages, which may indicate error conditions such as dropped frames. The M330 stores up to 512 system error messages in volatile memory (RAM). You can view these events using the M330 management tool, and you can configure M330 to relay them as syslog messages to a syslog server residing on the network.

You can also configure the M330 to store up to 512 messages in nonvolatile memory (flash). When full, the oldest log message gets overwritten by the new log message. Logged messages often indicate severe errors in M330 operation, and they may prove useful in diagnosing system crashes. All log messages are time stamped.

To configure system log settings, and view a limited number of log messages from RAM, select **Tools > System Log**.

System log configuration

You can use the **System log configuration** section of the System Log page to configure the size of the system log and specify which system events result in messages to store in the log, based on their severity level.



You can configure the following log settings:

Persistence

If the system unexpectedly reboots, log messages can be useful to diagnose the cause. However, log messages in volatile memory are lost when the system reboots. You can enable persistent logging to store log messages in flash memory so that they are retained after a reboot.

Choose **Enable** to save system logs to flash memory. Choose **Disable** to save system logs to volatile memory only.

Caution

Persistent logging can eventually wear out the flash memory and degrade network performance. You should only enable persistent logging to debug a problem. Make sure you disable persistent logging after you finish debugging the problem.

Severity

Specify the severity level of the log messages to write to the system log(s). This setting applies to messages stored in RAM and flash. In the following list, the severity levels are listed from most severe (top) to least severe (bottom):

- **Emergency** indicates that the system is unusable. It is the highest level of severity.
- **Alert** indicates action must be taken immediately.
- **Critical** indicates critical conditions.
- **Error** indicates error conditions.
- **Warning** indicates warning conditions.
- **Notice** indicates normal but significant conditions.
- **Informational** indicates informational messages.
- **Debug** indicates debug-level messages.

For example, if you specify **Critical**, then only critical, alert, and emergency messages are written to the log(s).

Depth

RAM and flash memory can store up to 512 messages each. When the depth value you configure is reached, the oldest log message is overwritten by the new log message.

Remote syslog configuration

You can view up to 512 messages stored in RAM in the **Events** section of the System Log page. To view a longer history of messages, you must set up a remote syslog server that acts as a syslog log relay host on your network. Then, you can configure the M330 to send syslog messages to the remote server. The **Severity** level setting configured in the **System log configuration** section determines which messages are stored in RAM and are available for relay to a remote syslog server.

Using the remote syslog feature provides these benefits:

- Allows aggregation of syslog messages from multiple M330s. The MAC address of the sending AP displays at the start of each message.
- Stores a longer history of messages than those that are kept on a single M330.
- Can trigger scripted management operations and alerts.

The procedure for configuring a remote log host depends on the type of system you use as the remote host.

You can use the **Remote syslog configuration** section of the System Log page to configure M330 remote log settings.

Remote syslog configuration

Remote syslog

☐ Enable ☒ Disable

Syslog server

Syslog port

(1 - 65535)

Save

Cancel

Remote syslog

Use this setting to enable or disable this feature. When enabled, messages of the selected **Severity** level or higher are sent to the configured syslog server. When disabled, a limited number of these messages will be stored locally and can be viewed in the **Events** section of the System Log page.

Syslog server

Specify the IP address or DNS name of the remote log server.

Syslog port

The syslog process uses logical port 514 by default. HP recommends that you keep this default. If you specify a different port number, ensure that the port number is not being used by another protocol on your network and that your syslog server is also configured to use that port.

Events

The **Events** section of the System Log page shows real-time system events on the AP, such as wireless clients associating with the AP and being authenticated. The log shows the date the event occurred, its severity level, the software program or process that caused the event message, and the message text.

You can click **Refresh** to display the most recent data from the AP, or **Clear All** to remove all entries from the list.

Email alert

The Email alert feature allows the AP to automatically send email messages when an event at or above the configured severity level occurs. To configure email alert settings, select **Tools > Email Alert**.

General configuration



Email Alert	
General	
Email alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
From address	<input type="text"/>
Urgent message severity	<input type="text" value="Alert"/>
Non urgent severity	<input type="text" value="Warning"/>
Log duration	<input type="text" value="30"/> (30 - 1440 minutes)

Email alert

Globally enable or disable the Email alert feature. It is disabled by default.

From address

Specify the email address that appears in the From field of alert messages sent from the AP, for example AP23@company.com. HP recommends that you use an email address that exists on your own network, so that the address will receive a notification if an email from the AP is undeliverable, and to prevent spam filters on the network from blocking the sending or delivery of emails from the AP.

The address can be a maximum of 255 characters and can contain only printable characters. By default, no address is configured.

Urgent message severity

This setting determines the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately upon being generated. The security level you select and all higher levels are considered urgent:

- **Emergency** indicates that the system is unusable. It is the highest level of severity.
- **Alert** indicates action must be taken immediately.
- **Critical** indicates critical conditions.
- **Error** indicates error conditions.
- **Warning** indicates warning conditions.
- **Notice** indicates normal but significant conditions.
- **Informational** indicates informational messages.
- **Debug** indicates debug-level messages.

Non-urgent severity

This setting determines the severity level for log messages that are considered to be non-urgent. Messages in this category are collected and sent in a digest form at the time interval specified by the **Log duration**. The security level you select and all levels up to but not including the lowest urgent level are considered non-urgent. Messages below the security level you specify are not sent via email.

See the **Urgent message severity** description for information about the security levels.

Log duration

This setting determines how frequently the non-urgent messages are sent to the email (SMTP) server. The range is 30 to 1440 minutes. The default is 30 minutes.

Non-urgent messages are sent when the time duration is reached or the number of messages exceeds the configured **Depth** value on the System Log page, whichever is first.

Mail server configuration

Mail server	
Mail server address	<input type="text"/>
Mail server security	Open ▼
Mail server port	25 (0 - 65535)

Mail server address

Specify the IP address or hostname of the SMTP server on the network.

Mail server security

Specify whether to use SMTP over SSL (**TLSv1**) or no security (**Open**) for authentication with the mail server. The default is **Open**.

Mail server port

Configure the TCP port number for SMTP. The range is a valid port number from 0 to 65535. The default is 25, which is the standard port for SMTP.

Username

This field displays only when **TLSv1** is selected as the **Mail server security** setting. Specify the username to use for authentication with the mail server. The username can be up to 64 characters long and can include any printable characters.

Password

Specify the password associated with the username configured in the previous field.

Message configuration

Message	
To address 1	<input type="text"/>
To address 2	<input type="text"/>
To address 3	<input type="text"/>
Email subject	Log message from AP
<input type="button" value="Test Mail"/> <input type="button" value="Save"/>	

To address 1/2/3

Configure the first email address to which alert messages are sent and, optionally, a second and third email address. The address must be in email address format, for example abc@def.com. By default, no addresses are configured.

Email subject

Specify the text to be displayed in the subject of the email alert message. The subject can contain up to 255 alphanumeric characters. The default is **Log message from AP**.

Sending a test message

To validate the configured email server credentials, select **Test Mail**.

The following text shows an example of an email alert sent from the AP to the network administrator:

```
From: AP-192.168.1.1@mailserver.com
Sent: Wednesday, February 08, 2015 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP
```

TIME	Priority	Process Id	Message
Feb 8 03:48:25	info	login[1457]	root login on 'ttyp0'
Feb 8 03:48:26	info	mini_http-ssl[1175]	Max concurrent connections of 20 reached

Viewing email alert status

You can select **Status > Email alert** to view the status of the email alert feature and information about past activity.

Email Alert

?

Email alert status

Email alert statusdownNumber of email sent0Number of email failed0Time since last email sent

Refresh

Email alert status

Indicates whether the Email alert feature is administratively enabled or disabled.

Number of emails sent

The number of alert emails sent since the feature was enabled.

Number of emails failed

The number of alert emails sent since the feature was enabled that did not reach the intended destination.

Time since last email sent

The date and time of the last alert email sent.

Network trace configuration

Overview

Network administrators can perform network traces to capture and analyze network traffic. Network trace operates in two modes:

- **Packet file trace mode:** Captured packets are stored in a file on the M330. The M330 can transfer the file to a TFTP server. The file is formatted in pcap format and can be examined using tools such as Wireshark and OmniPeek.
- **Remote packet trace mode:** The captured packets are redirected in real time to an external PC running the Wireshark tool.

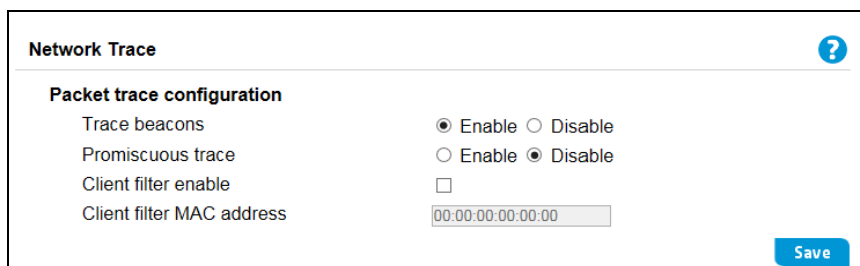
The AP can trace the following types of packets:

- 802.11 packets received and transmitted on radio interfaces. Packets captured on radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted within wireless communities or on internal logical interfaces, such as WDS interfaces.

To configure network trace settings and initiate packet captures, select **Tools > Network Trace**.

Packet trace configuration

Use this section to configure parameters that affect how packet trace functions on the radio interfaces.



Network Trace	
Packet trace configuration	
Trace beacons	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Promiscuous trace	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Client filter enable	<input type="checkbox"/>
Client filter MAC address	<input type="text" value="00:00:00:00:00:00"/>
<button>Save</button>	

Trace beacons

Enable to trace the 802.11 beacons detected or transmitted by the radio. HP recommends that you also enable **Promiscuous trace** when performing a beacon trace.

Promiscuous trace

Enable to place the radio in promiscuous mode when the trace is active.

In promiscuous mode, the radio receives all traffic on the channel, including traffic that is not destined to the M330. While the radio is operating in promiscuous mode, it continues serving associated clients. Packets not destined to the AP are not forwarded.

As soon as the trace is completed, the radio reverts to non-promiscuous mode operation.

Client filter enable

Enable to use the WLAN client filter to trace only frames that are transmitted to, or received from, a WLAN client with a specified MAC address.

Client filter MAC address

Specify a MAC address for WLAN client filtering. Note that the MAC filter is active only when a trace is performed on an 802.11 interface.

Note

Changes to packet trace settings take effect after a packet trace is restarted. Modifying the parameters while a packet trace is running does not affect the current packet trace session. To begin using new parameter values, an existing packet trace session must be stopped and restarted.

Packet file trace

In packet file trace mode, the M330 stores captured packets in a file on the device.

Upon activation, the packet trace proceeds until one of the following occurs:

- The trace time reaches configured duration.
- The trace file reaches its maximum size.
- The administrator stops the trace.

During the trace, you can monitor the trace status, elapsed trace time, and the current trace file size. You can click **Refresh** to update this information while the trace is in progress.

Performing a packet file trace

To perform a packet file trace.

1. Select **Tools > Network Trace**.

Packet file trace	
Trace interface	radio1 ▾
Trace duration	60 (10 - 3600 seconds)
Max trace file size	1024 (64 - 4096 KB)
<div>Start Trace Save</div>	

2. Select a **Trace interface**. The following M330 interfaces are available for packet trace:

- **radio1**: 802.11 traffic on the 2.4 GHz radio.
- **radio2**: 802.11 traffic on the 5 GHz radio.
- **eth0**: 802.3 traffic on the Ethernet port.
- **wlan0**: Traffic for the default wireless community on the 2.4 GHz radio.
- **wlan1**: Traffic for the default wireless community on the 5 GHz radio.
- **wlan0vapx**: Traffic for 2.4 GHz wireless community x, where x is the community ID and can be from 1 to 7. Wireless community IDs are shown in the first column of the Communities table on the **Wireless > Communities** page.

- **wlan1vapx**: Traffic for 5 GHz wireless community x, where x is the community ID and can be from 1 to 7. Wireless community IDs are shown in the first column of the Communities table on the **Wireless > Communities** page.
 - **brtrunk**: Traffic that is forwarded among different wireless communities, the Ethernet interface, and WDS interfaces.
 - **wlan0wdsx**: Traffic for 2.4 GHz WDS interface x, where x is the WDS interface ID and can be from 1 to 4. Configured WDS interfaces are shown on the **Wireless > WDS** page.
 - **wlan1wdsx**: Traffic for 5 GHz WDS interface x, where x is the WDS interface ID and can be from 1 to 4. Configured WDS interfaces are shown on the **Wireless > WDS** page.
3. Specify the following parameters:
- **Trace duration**: The time duration in seconds for the trace (range 10 to 3600).
 - **Max trace file size**: The maximum allowed size for the trace file in KB (range 64 to 4096).

If you change either of these values, you must click **Save** before initiating a trace.

4. Click **Start Trace**.

The trace session will run for the specified duration. You can view the trace status in the **Packet trace status** section. Click **Refresh** to see updated trace time and file size values. You can also click **Stop Trace** to stop a trace before the specified duration has elapsed.

Remote packet trace

Remote packet trace enables you to specify a remote port as the destination for packet captures. This feature works in conjunction with the Wireshark network analyzer tool for Windows. A packet trace server runs on the M330 and sends the captured packets via a TCP connection to the Wireshark tool.

A Windows PC running Wireshark enables you to display, log, and analyze captured traffic.

When the remote trace mode is in use, the M330 does not store any captured data locally in its file system.

Setting up Wireshark sessions

You can trace up to five interfaces on the M330 at the same time. However, you must start a separate Wireshark session for each interface. You can configure the IP port number used for connecting Wireshark to the M330. The default port number is 2002. The system uses five consecutive port numbers starting with the configured port for the packet trace sessions.

If a firewall is installed between the Wireshark PC and the M330, these ports must be allowed to pass through the firewall. The firewall must also be configured to allow the Wireshark PC to initiate TCP connection to the M330.

To configure Wireshark to use the M330 as the source for captured packets, you must specify the remote interface in the Capture Options menu. For example, to trace packets on an M330 with IP address 192.168.1.10 on radio 1 using the default IP port, specify the following interface:

```
rpcap://192.168.1.10/radio1
```

To trace packets on the Ethernet interface of the M330 and on the default wireless community (wlan0) using IP port 58000, start two Wireshark sessions and specify the following interfaces:

```
rpcap://192.168.1.10:58000/eth0  
rpcap://192.168.1.10:58000/wlan0
```

When you are capturing traffic on the radio interface, you can disable beacon trace, but other 802.11 control frames are still sent to Wireshark. You can set up a display filter to show only the following:

- Data frames in the trace
- Traffic on specific BSSIDs
- Traffic between two clients

Some examples of useful display filters are the following:

- Exclude beacons and ACK/RTS/CTS frames:

```
!(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)
```

- Data frames only:

```
wlan.fc.type == 2
```

- Traffic on a specific BSSID:

```
wlan.bssid == 00:02:bc:00:17:d0
```

- All traffic to and from a specific client:

```
wlan.addr == 00:00:e8:4e:5f:8e
```

Performance and security considerations

In remote packet trace mode, traffic is sent to the PC running Wireshark via one of the network interfaces. Depending on where the Wireshark tool is located, the traffic can be sent on an Ethernet interface or one of the radios. To avoid a traffic flood caused by tracing the trace packets, the M330 automatically installs a trace filter to filter out all packets destined to the Wireshark application. For example, if the Wireshark IP port is configured to be 58000, then the following trace filter is automatically installed on the M330:

```
not portrange 58000-58004
```

Enabling the packet trace feature impacts M330 performance and can create a security issue (unauthorized clients may be able to connect to the AP and trace user data). The M330 performance is negatively impacted even if there is no active Wireshark session with the AP. The performance is negatively impacted to a greater extent when packet trace is in progress.

Due to performance and security issues, the packet trace mode is not saved in nonvolatile memory on the M330. If the M330 resets, the trace mode is disabled and you must re-enable it to resume capturing traffic. Packet trace parameters (other than mode) are saved in nonvolatile memory.

To minimize any performance impact on the M330 while traffic trace is in progress, you should install trace filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, a large portion of the captured frames tend to be beacons (typically sent every 100 ms by all APs). Although Wireshark supports a display filter for beacon frames, it does not support a trace filter to prevent the M330 from forwarding captured beacon packets to the Wireshark tool. To reduce the performance impact of capturing the 802.11 beacons, you can disable the trace beacons mode.

The remote packet trace facility is a standard feature of the Wireshark tool for Windows.

Note

Remote packet trace is not standard on the Linux version of Wireshark. The Linux version does not work with the AP.

Wireshark is an open source tool and is available for free. It can be downloaded from www.wireshark.org.

Performing a remote packet trace

To perform a remote packet trace.

1. Set up the Wireshark session as described in “[Setting up Wireshark sessions](#)” on [page 129](#).
2. On the M330 management tool, select **Tools > Network Trace**.

Remote packet trace
Remote capture port (1025 - 65530)
Start Remote Trace Save

3. In the **Remote packet trace** section, specify the Remote trace port. Specify the remote port to use as the destination for packet captures. The range is 1 to 65530 and the default port is 2002. If you change this value, you must click **Save** prior to starting the remote trace.
4. Select **Start Remote Trace**.

The trace session will run for the specified duration. You can view the trace status in the **Packet trace status** section. Click **Refresh** to see the updated trace time. You can also click **Stop Trace** to stop a trace before the specified duration has elapsed.

Packet trace status

This section enables you to view the status of the packet trace on the AP.

Packet trace status

Current trace status	Not started
Packet trace time	00:00:00
Packet trace file size	0 KB

Stop Trace Refresh

Current trace status

Whether a packet trace is running or is stopped.

Packet trace time

The elapsed trace time for a trace in progress.

Packet trace file size

The current trace file size.

Packet trace file download

This section enables you to download the trace file by TFTP to a configured TFTP server, or by HTTP(S) to a PC. A trace is automatically stopped when the trace file download command is triggered.

HTTP download

Select **HTTP** to download to your PC or a network location.

Packet trace file download	
Download method	<input checked="" type="radio"/> HTTP <input type="radio"/> TFTP
TFTP server filename	<input type="text" value="apcapture.pcap"/>
Server IP	<input type="text" value="0.0.0.0"/>
<input type="button" value="Download"/>	

When you select **Download**, you will be able to browse to the desired location.

TFTP download

Select **TFTP** to download to download to a TFTP server.

Packet trace file download	
Download method	<input type="radio"/> HTTP <input checked="" type="radio"/> TFTP
TFTP server filename	<input type="text" value="apcapture.pcap"/>
Server IP	<input type="text" value="0.0.0.0"/>
<input type="button" value="Download"/>	

TFTP server filename

The file will be saved to the TFTP server under this name and path.

Server IP

Enter the IP address of the TFTP server.

When you click **Download**, a progress bar displays to indicate download status.

Ping

The M330 supports ping functionality to enable basic diagnostics of network devices. To ping another device, select **Tools > Ping**.



The screenshot shows a web-based interface for the Ping utility. It has a title bar with the word "Ping" and a question mark icon. Below the title bar, there are three input fields: "Address to ping" (empty), "Timeout" (set to 5), and "Result" (empty). The "Timeout" field has a range "(1 - 15 seconds)" next to it. A "Start" button is located at the bottom right of the form.

Address to ping

You can specify an IPv4 address, an IPv6 address, or a hostname.

Timeout

Specify the amount of time in seconds after which an unsuccessful ping will time out.

Results

The results window shows the size and number of each packet sent and, if the host is reached, the size and number of each packet received in response and its round-trip time. It also displays statistics about packet loss and, if the host is reached, the average round-trip time for all packets.

12 Support and other resources

Online documentation

You can download documentation from the HP Support Center website www.hp.com/support/manuals. Search by product number or name.

Contacting HP

For worldwide technical support information, see the HP Networking Support website: www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Problem description and any detailed questions

HP websites

For additional information, see the following HP websites:

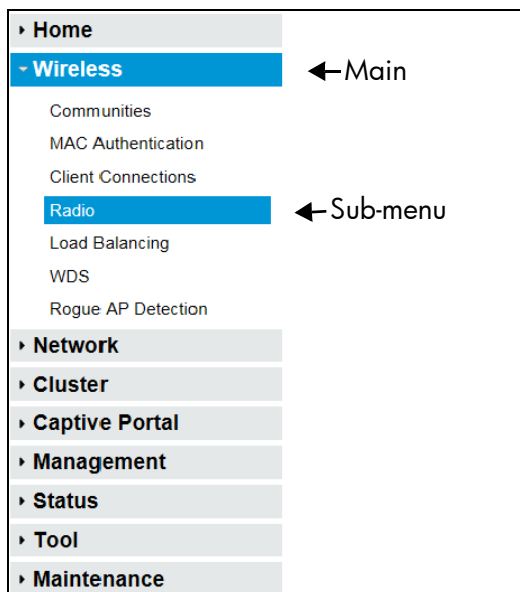
- www.hp.com/networking
- www.hp.com

Conventions

The following conventions are used in this guide.

Management tool

This guide uses specific syntax when directing you to interact with the web management user interface. Refer to the following image for identification of key user-interface elements and then the table below for example directions:



Example directions in this guide	What to do in the user interface
Select Wireless > Radio .	Select Wireless on the main menu, and then select Radio on the sub-menu.
Set Mode to IEEE 802.11 n/ac .	For the Mode setting, select the IEEE 802.11 n/ac from the list.

A Resetting to factory defaults

Factory reset procedures

To force the M330 into its factory default state, follow the procedures in this section.

Caution

Resetting the M330 to factory defaults deletes all configuration settings, resets the manager user name and password to **admin**, and enables the DHCP client on the Ethernet port. If no DHCP server assigns an address to the M330, its address defaults to 192.168.1.1.

Using the reset button

Using a tool such as a paper clip, press and hold the reset button for a few seconds until the status lights blink three times.

Using the management tool

To reset the M330 to factory defaults:

1. Launch the management tool (default <https://192.168.1.1>).
2. Select **Maintenance > Config File Management**.
3. Under **Reset**, click **Reset**.

