ELTEXALATAU
Complete solutions for networking

WEP-12ac, WOP-12ac

Operation Manual
Device control via WEB-configurator,Firmware Version 1.6.4
(05.2016)

Wireless Access Point

IP-address: http://192.168.1.10

user name: admin

password: password

www.eltexalatau.kz

Document version	Issue date	Revisions
Versoin 1.4	17.05.2016	Synchronized with firmware version 1.6.4 Changes in chapters: - 5.4 «Wireless Settings» submenu - 5.5 «Radio» submenu
Versoin 1.3	26.02.2016	Synchronized with firmware version 1.6.3 Changes in chapters: - 5.5 «Radio» submenu - 5.8 «VAP» submenu - 11.1 «Global Configuration» submenu - 11.2 «Instrance Congiguration» submenu
Versoin 1.2	14.10.2015	Synchronized with firmware version 1.6.2 Added chapters: - 5.9 "VAP Minimal Signal" submenu - 5.10 "Fast Bss Transition" submenu Changes in chapters: - 4.5 «Client Associations» submenu - 5.5 "Wireless Settings" submenu - 5.5 "Radio" submenu - 5.8 "VAP" submenu - 6.2 «Web Server» submenu - 6.8 «SNMP» submenu - 8.1 «Configuration» submenu - 10.1 «Access Points» submenu - 11.2 «Instance Configuration» submenu - 12.1 «VAP QoS Parametrs» submenu - 12.3 «Policy Map» submenu - 13.1 «Work group bridge» submenu
Versoin 1.1	26.03.2015	Synchronized with firmware version 1.5.0. Added chapters: - 4.4 «Wireless Multicast Forwarding Statistic» submenu - 5.10 «Wireless Multicast Forwarding» submenu - 10.5 «Cluster Firmware Upgrade» submenu - 12.4 «Client Configuration» submenu Changes in chapters: - 4.3 «Transmit/Receive» submenu - 4.5 «Client Associations» submenu - 4.6 «Rogue AP Detection» submenu - 5.8 «VAP» submenu - 5.10 «WDS» submenu - 10.1 «Access Points» submenu - 11.2 «Instance Configuration» submenu - 13.1 «Work group bridge» submenu
Versoin 1.0	23.09.2014	First issue.
Firmware Version	**1.6.3**	

CONTENTS

1 INTRODUCTION

1.1 Annotasion

The manual addendam provides information about the device structure of the web interface, basic skills of the interface surfing, rules of configuring, monitoring and software changing of the wireless hot spot (hereinafter referred to as the device).

Web-interface allows you to make a device management more visual and comfortable. Configurating, monitoring, device debugging from the remote work place are realized by web-browser.

1.2 Targated audience

Web-interface is destined for technical staff which realizes tuning and monitoring of the wireless hot spot by the web-interface (hereinafter referred to as the device). Technical staff qualification supposes knowledges of the basic operation with the TCP/IP, UDP/IP protocols and design concept of Ethernet- and wireless network.

1.3 Symbols

Value	*Description*
Semibold italic	Notes and warnings are written in semibold font.
Italic	Information for special attention is assigned by italic.

Notes and warnings

✓ **Notes contain important information, tips or recommendations on device operation and setup.**

! **Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.**

2 WEB-INTERFACE DESCRIPTION

2.1 Startup

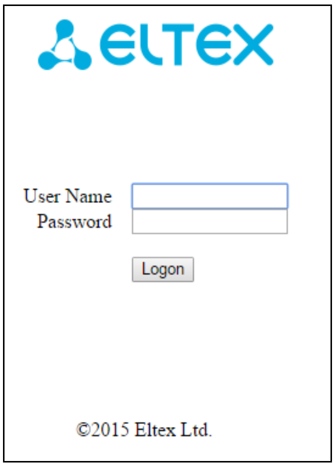
You should be connected to the device via Web-browser for startup:

1. Open Web-browser (web-page explorer), for example, Firefox, Opera, Chrome.
2. Enter IP-address of the device to the browser address line.

Default IP-address of the device: 192.168.1.10, Subnet mask: 255.255.255.0

Default device configuration gets address through DHCP. Befor that, the device is available by default IP-address.

If connection is successful, request form with user name and password will be displaed on the browser window.



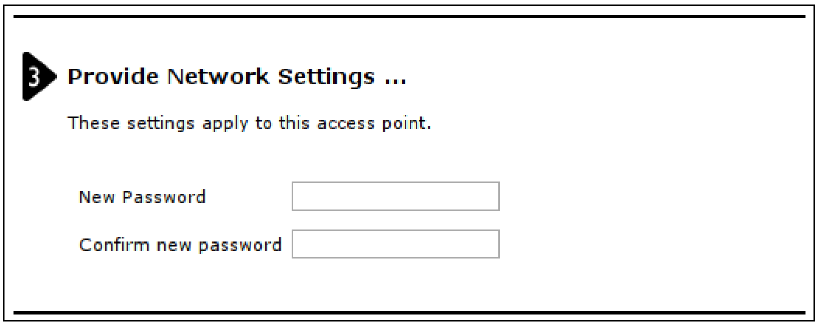
3. Enter the user name in the «User Name» line and password in the «Password» line.

Factory settings: user name: *admin*, password: *password*.

4. Click **Logon** button. Device web-configurator home page will be opened in the browser window.

2.2 Password reset

Enter new password in the «New Password» and «Confirm new password» fields to change a password of the connection to the device web-configurator.

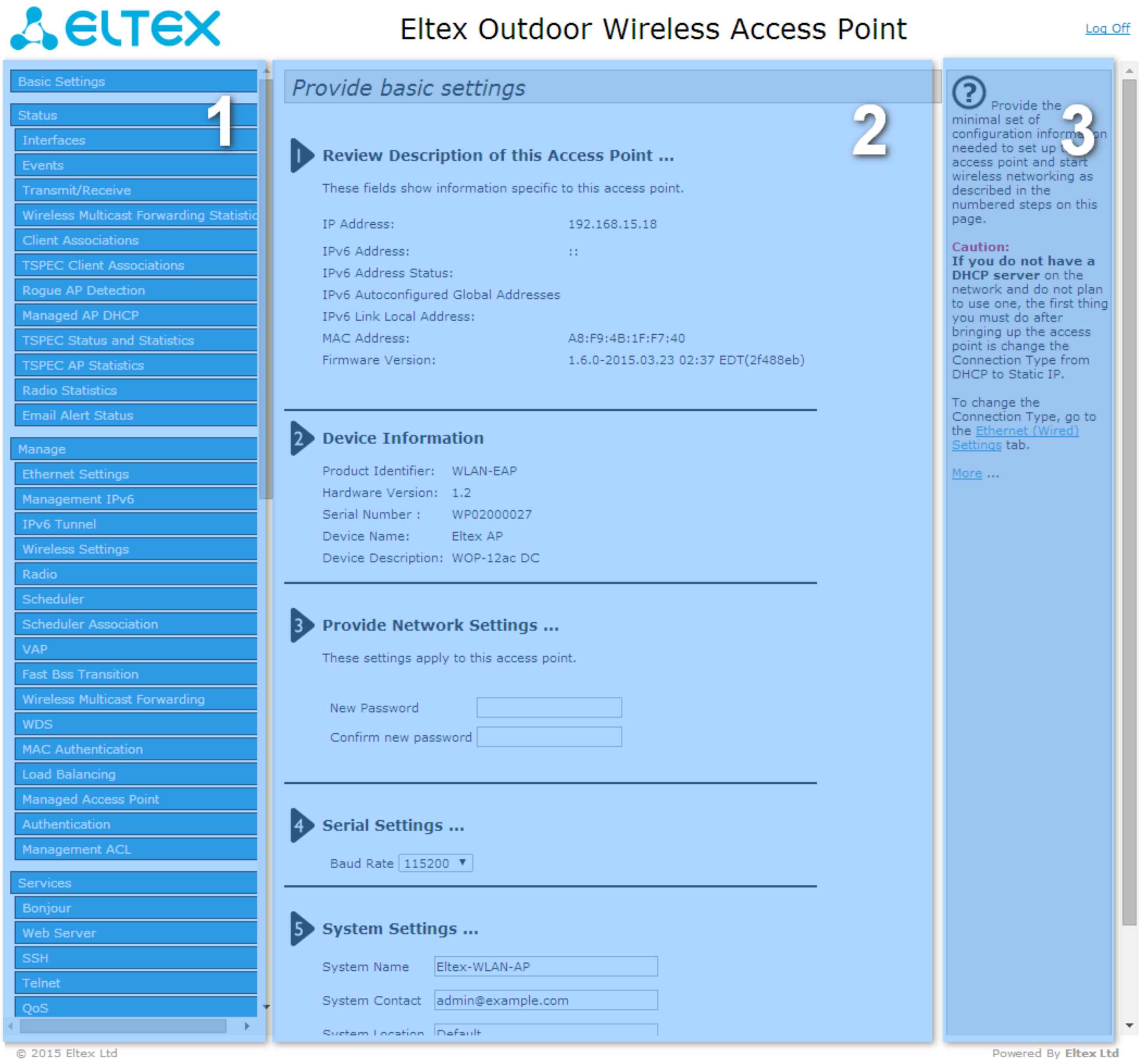


Provide Network Settings ...

These settings apply to this access point.

2.3 WEB-configurator elements

Fig. 1 shows web-confogurator navigation elements.



Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 192.168.15.18
IPv6 Address: ::
IPv6 Address Status:
IPv6 Autoconfigured Global Addresses
IPv6 Link Local Address:
MAC Address: A8:F9:4B:1F:F7:40
Firmware Version: 1.6.0-2015.03.23 02:37 EDT(2f488eb)

2 Device Information

Product Identifier: WLAN-EAP
Hardware Version: 1.2
Serial Number : WP02000027
Device Name: Eltex AP
Device Description: WOP-12ac DC

3 Provide Network Settings ...

These settings apply to this access point.

New Password
Confirm new password

4 Serial Settings ...

Baud Rate 115200

5 System Settings ...

System Name Eltex-WLAN-AP
System Contact admin@example.com
System Location Default

Provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

Caution:
If you do not have a DHCP server on the network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the Ethernet (Wired) Settings tab.

More ...

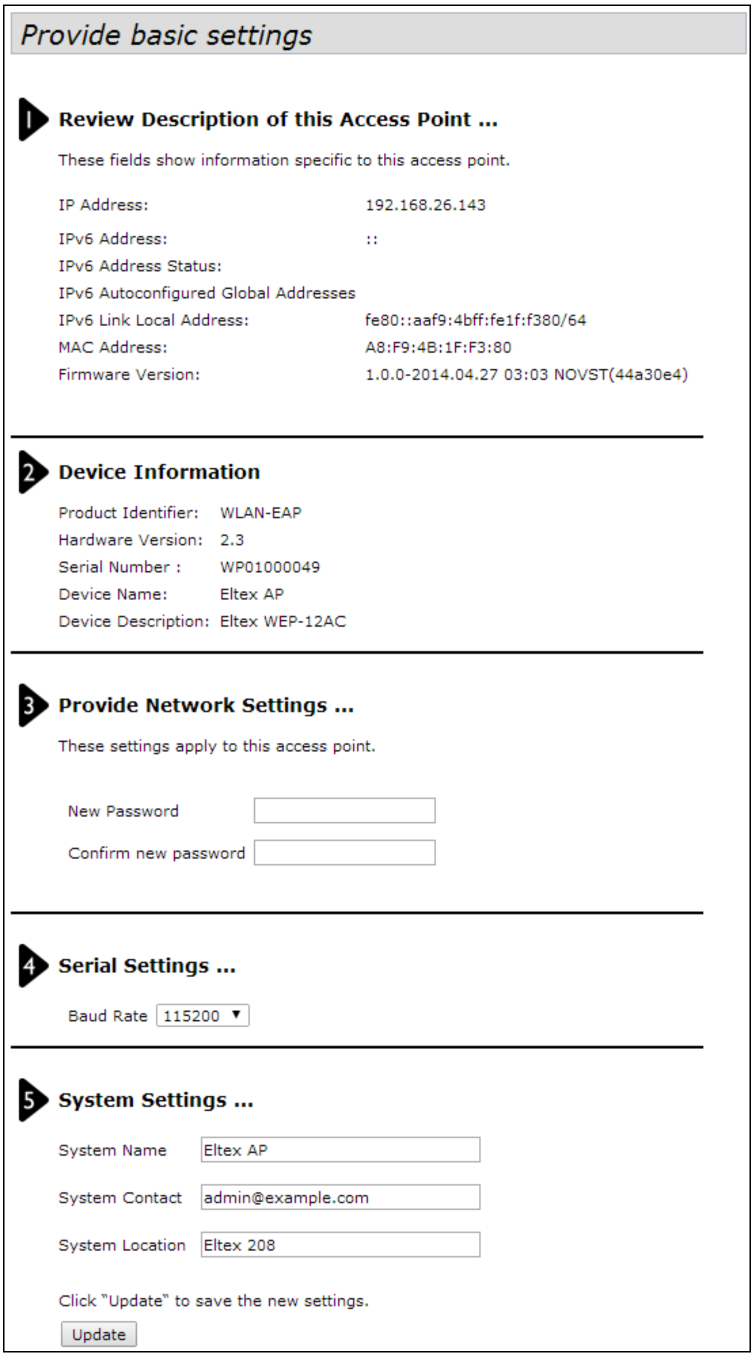
Fig. 1 – Web-confogurator navigation elements

User interface window can be devided into 3 parts:

1 Menu sections of the device settings.
2 Base window of the chosen section settings.
3 Background information about chosen section of the menu.

3 «BASIC SETTINGS» MENU

From the **Basic Settings** page, you can view various information about the UAP, including IP and MAC address information, and configure the administrator password for the UAP.



Provide basic settings

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address:	192.168.26.143
IPv6 Address:	::
IPv6 Address Status:	
IPv6 Autoconfigured Global Addresses	
IPv6 Link Local Address:	fe80::aaf9:4bff:fe1f:f380/64
MAC Address:	A8:F9:4B:1F:F3:80
Firmware Version:	1.0.0-2014.04.27 03:03 NOVST(44a30e4)

2 Device Information

Product Identifier:	WLAN-EAP
Hardware Version:	2.3
Serial Number :	WP01000049
Device Name:	Eltex AP
Device Description:	Eltex WEP-12AC

3 Provide Network Settings ...

These settings apply to this access point.

New Password

Confirm new password

4 Serial Settings ...

Baud Rate 115200

5 System Settings ...

System Name: Eltex AP

System Contact: admin@example.com

System Location: Eltex 208

Click "Update" to save the new settings.

Field	*Description*
IP Address	Shows the IP address assigned to the AP. This *Field* is not editable on this page because the IP address is already assigned (either by DHCP, or statically through the Ethernet Settings page).
IPv6 Address	Shows the IPv6 address assigned to the AP. This *Field* is not editable on this page because the IP address is already assigned (either by DHCPv6, or statically through the Management IPv6 page).
IPv6 Address Status	Shows the operational status of the static IPv6 address assigned to the management interface of the AP. The possible values are Operational and Tentative. **Note:** If an IPv6 address has not been manually configured or leased from a DHCPv6 server, the *Field* is blank.
IPv6 Autoconfigured Global Addresses	Shows each automatically-configured global IPv6 address for the management interface of the AP.
IPv6 Link Local Address	Shows the IPv6 Link Local address, which 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.
MAC Address	Shows the MAC address of the AP. The address shown here is the MAC address associated with the management interface. This is the address by which the AP is known externally to other networks.
Firmware Version	Shows version information about the firmware currently installed on the AP. As new versions of the WLAN AP firmware become available, you can upgrade the firmware on your APs.
Product Identifier	Identifies the AP hardware model.
Hardware Version	Identifies the AP hardware version.
Serial Number	Shows the AP serial number.
Device Name	Generic name to identify the type of hardware.
Device Description	Provides information about the product hardware.
New Password	Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type. The administrator password must be an string of up to maximum length of 32 characters. **Note:** As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.
Baud Rate	Select a baud rate for the serial port connection. The baud rate on the AP must match the baud rate on the terminal or terminal emulator to connect to the AP command-line interface (CLI) by using a serial (console) connection. The following baud rates are available:
System Name	Enter a name for the AP. This name appears only on the Basic Settings page and is a name to identify the AP to the administrator. The valid name is from 1 to 63 characters and can include letters, digits, hyphens and space, for example My AP.
System Contact	Enter the name, e-mail address, or phone number of the person to contact regarding issues related to the AP.

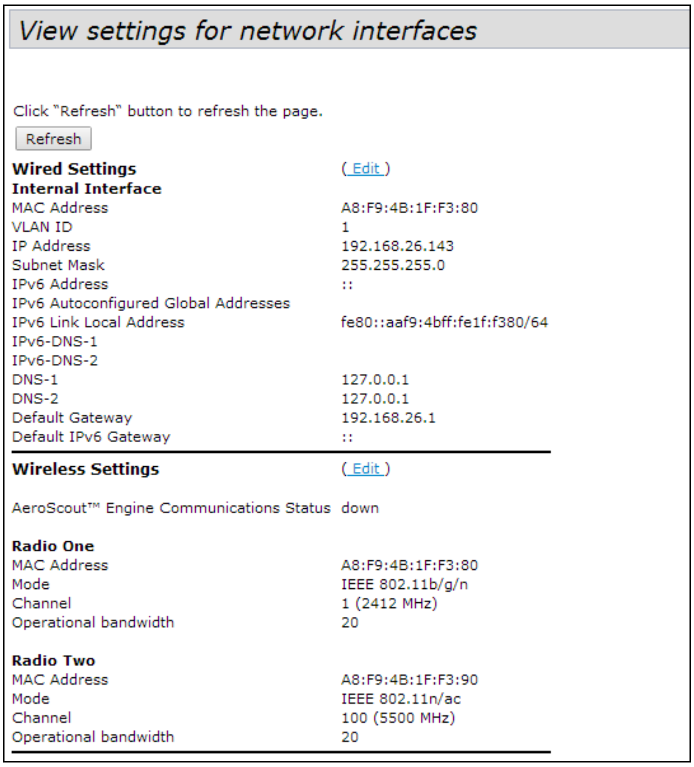
Click **Update** to save the new settings.

4 «STATUS» MENU

This page displays the current settings for the wired Ethernet interface and the wireless radio interfaces on the AP.

4.1 «Interfaces» submenu

The wired settings show information about the internal Ethernet interface, which is the primary interface used to manage the AP.



View settings for network interfaces

Click "Refresh" button to refresh the page.

Refresh

Wired Settings	(Edit)
Internal Interface	
MAC Address	A8:F9:4B:1F:F3:80
VLAN ID	1
IP Address	192.168.26.143
Subnet Mask	255.255.255.0
IPv6 Address	::
IPv6 Autoconfigured Global Addresses	
IPv6 Link Local Address	fe80::aaf9:4bff:fe1f:f380/64
IPv6-DNS-1	
IPv6-DNS-2	
DNS-1	127.0.0.1
DNS-2	127.0.0.1
Default Gateway	192.168.26.1
Default IPv6 Gateway	::
Wireless Settings	(Edit)
AeroScout™ Engine Communications Status	down
Radio One	
MAC Address	A8:F9:4B:1F:F3:80
Mode	IEEE 802.11b/g/n
Channel	1 (2412 MHz)
Operational bandwidth	20
Radio Two	
MAC Address	A8:F9:4B:1F:F3:90
Mode	IEEE 802.11n/ac
Channel	100 (5500 MHz)
Operational bandwidth	20

Wired Settings (Internal Interface)

Field	Description
MAC Address	The MAC address for the LAN interface for the Ethernet port on this AP. This is a read-only *Field* that you cannot change.
VLAN ID	The management VLAN ID. This is the VLAN associated with the IP address you use to access the AP management interface. The default management VLAN ID is 1.
IP Address	The IP address of the management interface.
Subnet Mask	The subnet mask associated with the management IP address.
IPv6 Address	The IPv6 address of the management interface.
IPv6 Autoconfigured Global Addresses	If the AP has been assigned one or more IPv6 addresses automatically, the addresses arelisted.
IPv6 Link LocalAddress	The IPv6 Link Local address, which 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-DNS-1 ***IPv6-DNS-2***	The primary and secondary DNS servers to use for name-to-IPv6 address resolution.
DNS-1 ***DNS-2***	The primary and secondary DNS servers to use for name-to-IP address resolution.
Default Gateway	The default gateway for the IPv4 network interface.
Default IPv6 Gateway	The default gateway for the IPv6 network interface.

To change the wired settings, click the **Edit** link. After you click **Edit**, you are redirected to the **Ethernet Settings** page.

Wireless Settings

The wireless settings show summary information about the radio interface configuration.

Field	***Description***
AeroScout™ Engine Communications Status	The status of the AeroScout protocol on the AP. When enabled, AeroScout devices are recognized and data is sent to an AeroScout Engine (AE) for analysis. The AE determines the geographical location of 802.11-capable devices, such as STAs, APs, and AeroScout's line of 802.11-enabled RFID devices, or *tags*. The AE communicates with APs that support the AE protocol in order to collect information about the RF devices detected by the APs.
Radio One and Radio Two	
MAC Address	The MAC addresses for the interface. This page shows the MAC addresses for Radio Interface One and Radio Interface Two. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.
Mode	The Physical Layer (PHY) standard the radio uses: IEEE 802.11b/g-802.11b and 802.11g clients can connect to the AP. IEEE 802.11b/g/n -802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the AP. 2.4 GHz IEEE 802.11n-Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.IEEE 802.11a-Only 802.11a clients can connect to the AP. IEEE 802.11a/n-802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 1.5 GHz IEEE 802.11n-Only 802.11n clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 1. IEEE 802.11a/n/ac-802.11a, 802.11n, and 802.11ac clients operating in the 5-GHzfrequency can connect to the AP. This mode is available only on Radio 2.IEEE 802.11n/ac-802.11n clients and 802.11ac clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 2.
Channel	The current operating channel. 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).
OperationalBandwidth	The size of the bandwidth, in MHz, the current channel is using.

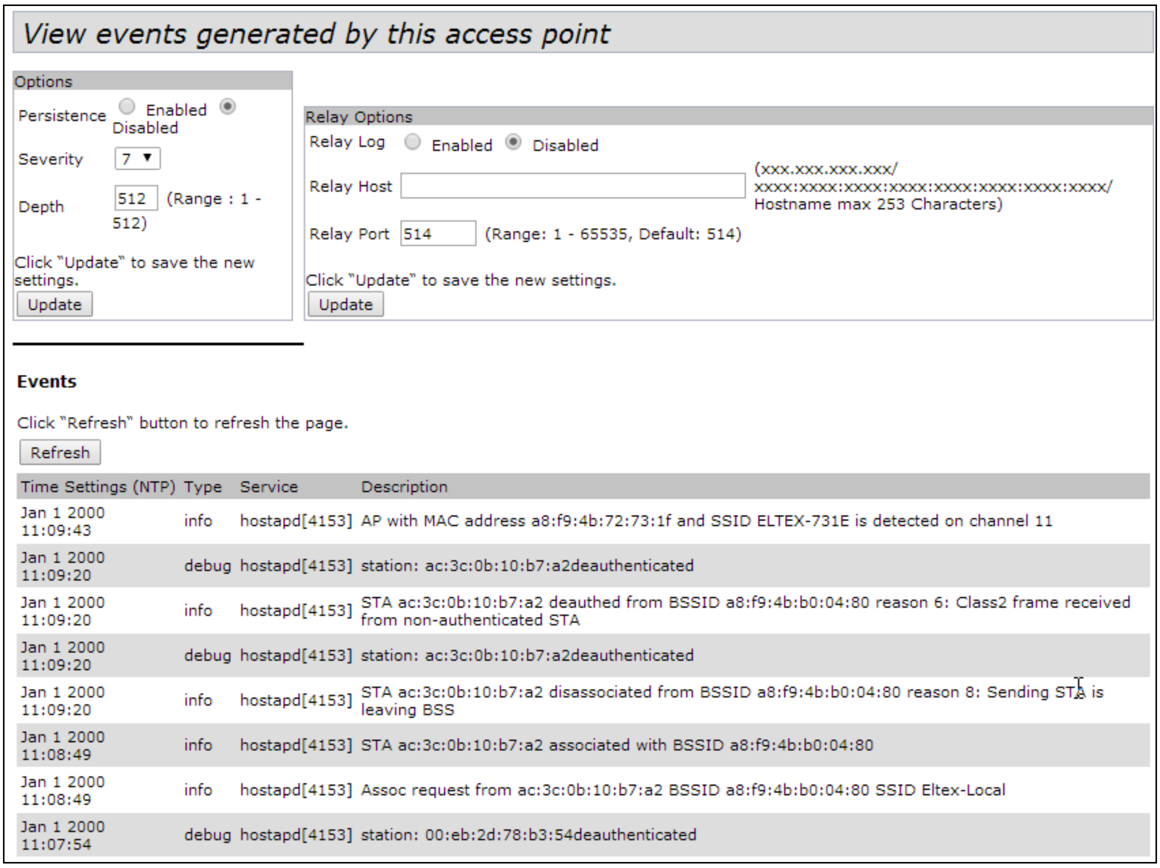
To change the radio mode or channel settings, click the **Edit** link. After you click **Edit**, you are redirected to the **Modify Wireless Settings** page.

Click **Refresh** button to refresh the page.

4.2 «Events» submenu

The Events page shows real-time system events on the AP such as wireless clients associating with the AP and being authenticated.

From the Events page, you can view the most recent events generated by this AP and configure logging settings. You can enable and configure persistent logging to write system event logs to non-volatile memory so that the events are not erased when the system reboots. This page also gives you the option of enabling a remote log relay host to capture all system events and errors in a Kernel Log.



View events generated by this access point

Options

Persistence ○ Enabled ● Disabled

Severity 7 ▼

Depth 512 (Range : 1 - 512)

Click "Update" to save the new settings.

Update

Relay Options

Relay Log ○ Enabled ● Disabled

Relay Host (xxx.xxx.xxx.xxx/ xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/ Hostname max 253 Characters)

Relay Port 514 (Range: 1 - 65535, Default: 514)

Click "Update" to save the new settings.

Update

Events

Click "Refresh" button to refresh the page.

Refresh

Time Settings (NTP)	Type	Service	Description
Jan 1 2000 11:09:43	info	hostapd[4153]	AP with MAC address a8:f9:4b:72:73:1f and SSID ELTEX-731E is detected on channel 11
Jan 1 2000 11:09:20	debug	hostapd[4153]	station: ac:3c:0b:10:b7:a2deauthenticated
Jan 1 2000 11:09:20	info	hostapd[4153]	STA ac:3c:0b:10:b7:a2 deauthed from BSSID a8:f9:4b:b0:04:80 reason 6: Class2 frame received from non-authenticated STA
Jan 1 2000 11:09:20	debug	hostapd[4153]	station: ac:3c:0b:10:b7:a2deauthenticated
Jan 1 2000 11:09:20	info	hostapd[4153]	STA ac:3c:0b:10:b7:a2 disassociated from BSSID a8:f9:4b:b0:04:80 reason 8: Sending STA is leaving BSS
Jan 1 2000 11:08:49	info	hostapd[4153]	STA ac:3c:0b:10:b7:a2 associated with BSSID a8:f9:4b:b0:04:80
Jan 1 2000 11:08:49	info	hostapd[4153]	Assoc request from ac:3c:0b:10:b7:a2 BSSID a8:f9:4b:b0:04:80 SSID Eltex-Local
Jan 1 2000 11:07:54	debug	hostapd[4153]	station: 00:eb:2d:78:b3:54deauthenticated

Field	Description
Persistence	Choose **Enabled** to save system logs to non-volatile memory so that the logs are not erased when the AP reboots. When persistence is enabled, we can store up to 128 messages in non-volatile memory. Choose **Disabled** to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
Severity	Specify the severity level of the log messages to be displayed. For example, if you specify 2, critical, alert, and emergency logs are displayed to the user. Error messages with a severity level of 3-7 are not displayed. 0-emergency 1-alert 2-critical 3-error 4-warning 5-notice 6-info 7-debug
Depth	You can store up to 512 messages in volatile memory. Once the number you configure in this *Field* is reached, the oldest log event is overwritten by the new log event.If persistence is enabled, on AP reboot it will show the old logs that are stored in the non-volatile memory, as the logs stored in the volatile memory will be erased.

Note: To apply your changes, click **Update**. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.**Enabling or Disabling the Log Relay Host on the Events Page.**

To enable and configure Log Relaying on the **Events** page, set the Log Relay options as described in the following table, and then click **Update.**

Field	Description
Relay Log	Select **Enabled** to allow the UAP to send log messages to a remote host. Select **Disabled**to keep all log messages on the local system.
Relay Host	Specify the IP Address or IPv6 Address or DNS name of the remote log server.
Relay Port	Specify the Port number for the syslog process on the Relay Host. The default port is 514.

Note: To apply your changes, click **Update**. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

If you enabled the Log Relay Host, clicking **Update** will activate remote logging. The AP will send its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

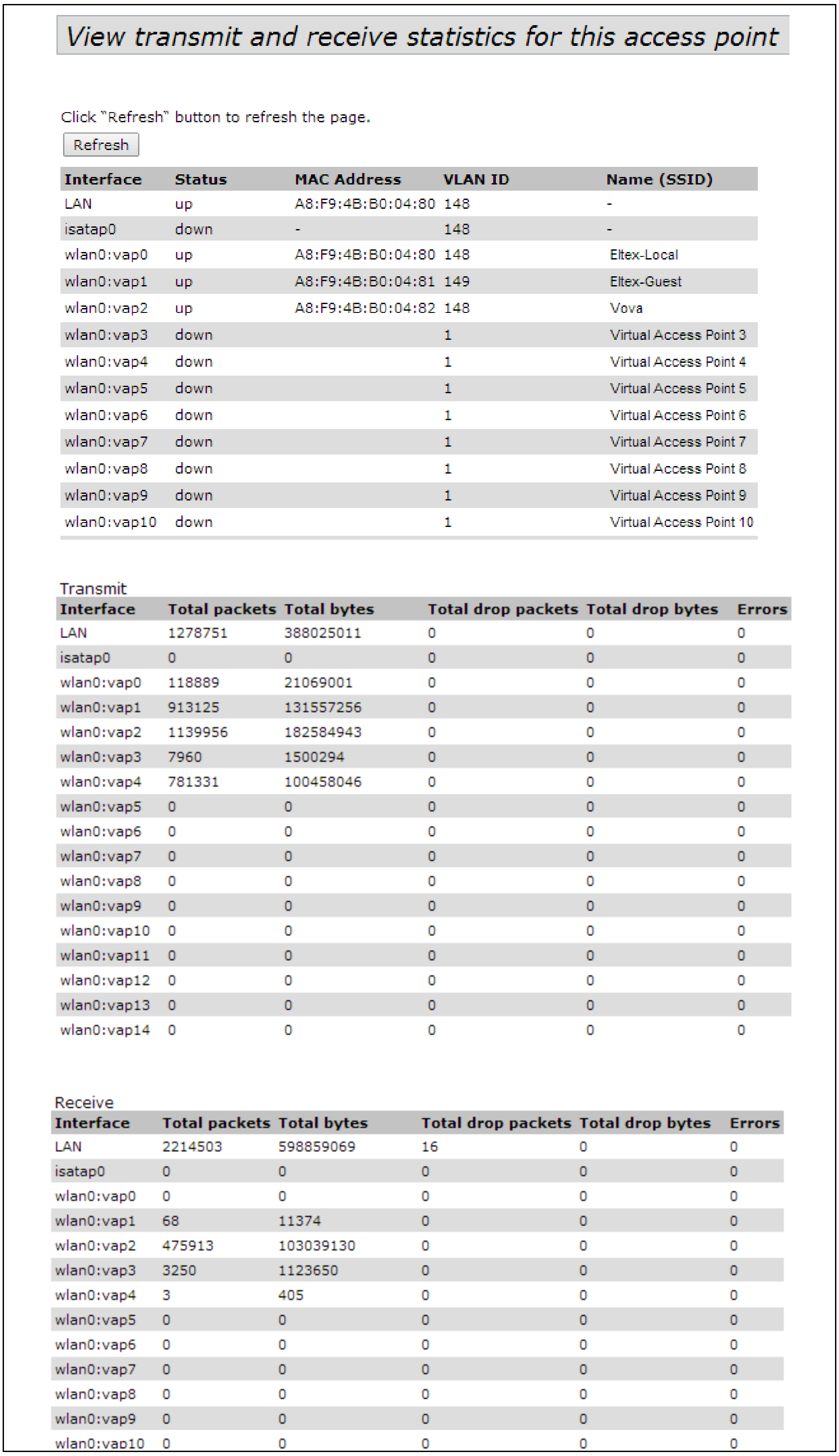
If you disabled the Log Relay Host, clicking **Update** will disable remote logging.

Click **Refresh** button to refresh the «Events» page.

Click **Clear All** to erase all events.

4.3 «Transmit/Receive» submenu

The **Transmit/Receive** page provides some basic information about the current AP and a real-time display of the transmit and receive statistics for the Ethernet,ISATAP interface on the AP and for the VAPs on both radio interfaces.



View transmit and receive statistics for this access point

Click "Refresh" button to refresh the page.

Refresh

Interface	Status	MAC Address	VLAN ID	Name (SSID)
LAN	up	A8:F9:4B:B0:04:80	148	-
isatap0	down	-	148	-
wlan0:vap0	up	A8:F9:4B:B0:04:80	148	Eltex-Local
wlan0:vap1	up	A8:F9:4B:B0:04:81	149	Eltex-Guest
wlan0:vap2	up	A8:F9:4B:B0:04:82	148	Vova
wlan0:vap3	down		1	Virtual Access Point 3
wlan0:vap4	down		1	Virtual Access Point 4
wlan0:vap5	down		1	Virtual Access Point 5
wlan0:vap6	down		1	Virtual Access Point 6
wlan0:vap7	down		1	Virtual Access Point 7
wlan0:vap8	down		1	Virtual Access Point 8
wlan0:vap9	down		1	Virtual Access Point 9
wlan0:vap10	down		1	Virtual Access Point 10

Transmit

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	1278751	388025011	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	118889	21069001	0	0	0
wlan0:vap1	913125	131557256	0	0	0
wlan0:vap2	1139956	182584943	0	0	0
wlan0:vap3	7960	1500294	0	0	0
wlan0:vap4	781331	100458046	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0

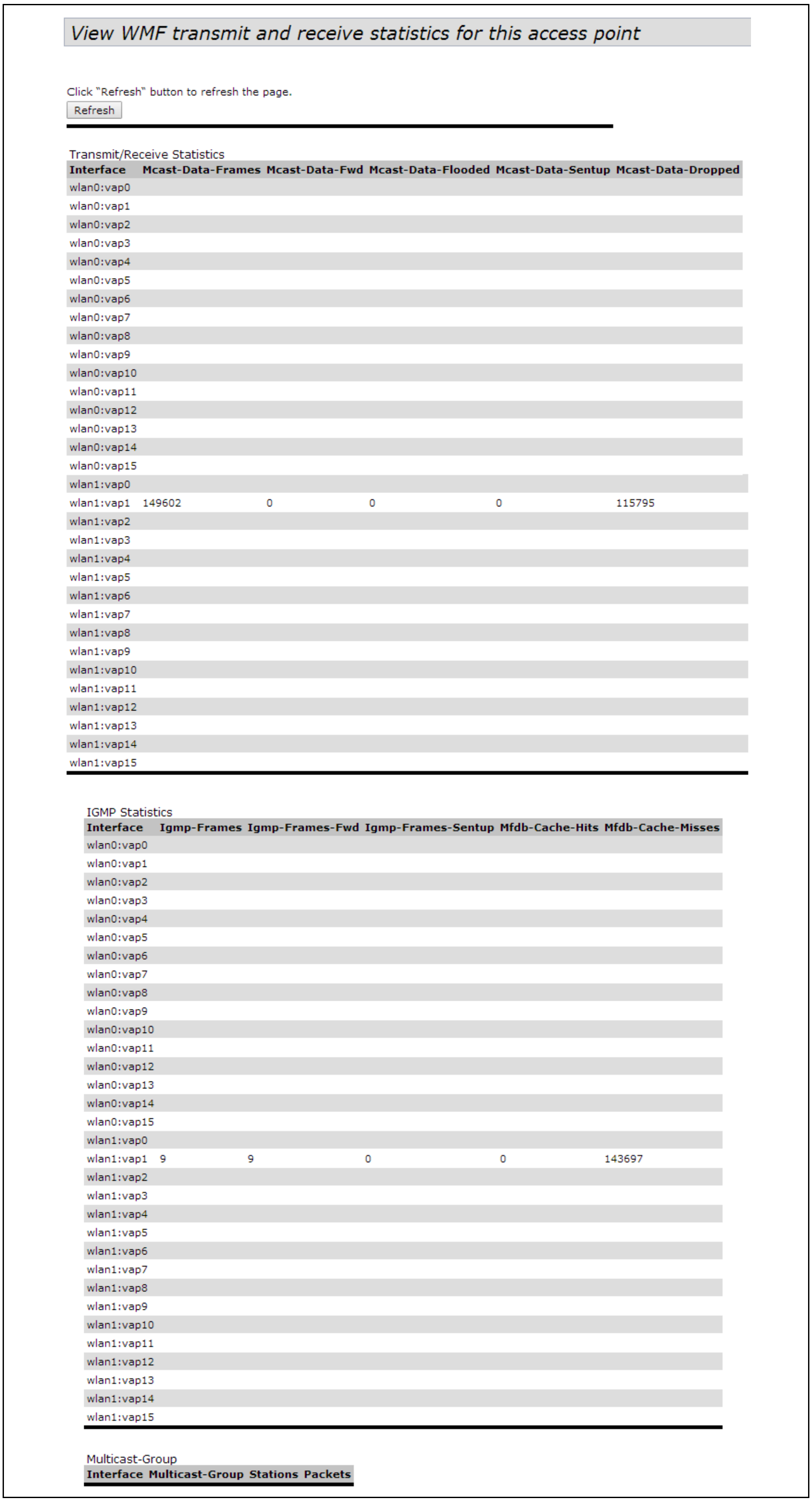
Receive

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	2214503	598859069	16	0	0
isatap0	0	0	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	68	11374	0	0	0
wlan0:vap2	475913	103039130	0	0	0
wlan0:vap3	3250	1123650	0	0	0
wlan0:vap4	3	405	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0

Field	Description
Interface	The name of the Ethernet,ISATAP or VAP interface.
Status	Shows whether the interface is up or down.
MAC Address	MAC address for the specified interface. The UAP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.
VLAN ID	Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same AP. The VLAN ID is set on the VAP tab.
Name (SSID)	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP tab.
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this AP.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this AP.
Total Drop Packets	Indicates total number of packets sent (in Transmit table) or received (in Received table) by this AP that were dropped.
Total Drop Bytes	Indicates total number of bytes sent (in Transmit table) or received (in Received table) by this AP that were dropped.
Transmit Errors	Indicates the errors related to sending the data on this AP. Typical errors include runt frames, frames destined to invalid stations, etc.
Receive Errors	Indicates the errors related to receiving the data on this AP. Typical Errors include runt frames, receive fifo overflow errors, bad src mac, etc.

4.4 «Wireless Multicast Forwarding Statistic» submenu

The **Wireless Multicast Forwarding Transmit and Receive Statistics** page provides some basic information about the current AP and a real-time display of the transmit and receive statistics for the Wireless Multicast Traffic interface on the AP and for the VAPs on both radio interfaces.



View WMF transmit and receive statistics for this access point

Click "Refresh" button to refresh the page.

Transmit/Receive Statistics

Interface	Mcast-Data-Frames	Mcast-Data-Fwd	Mcast-Data-Flooded	Mcast-Data-Sentup	Mcast-Data-Dropped
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	149602	0	0	0	115795
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

IGMP Statistics

Interface	Igmp-Frames	Igmp-Frames-Fwd	Igmp-Frames-Sentup	Mfdb-Cache-Hits	Mfdb-Cache-Misses
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	9	9	0	0	143697
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

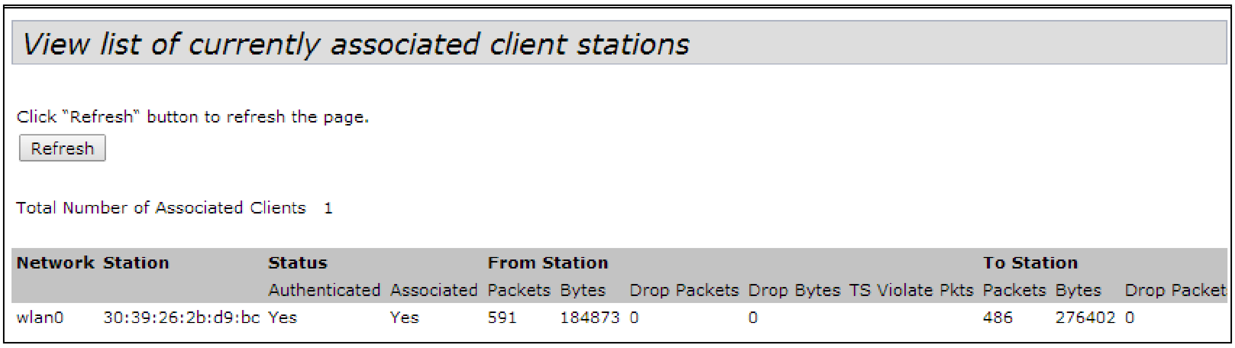
Multicast-Group

Interface	Multicast-Group	Stations	Packets

Field	*Description*
Transmit/Receive Statistics	
Interface	The name of the VAP interface.
Mcast-Data-Frames	Shows Multicast data frames received.
Mcast-Data-Fwd	Indicates Multicast data frames forwarded.
Mcast-Data-Flooded	Indicates Multicast data frames flooded.
Mcast-Data-Sentup	Indicates Multicast data frames sent up.
Mcast-Data-Dropped	Indicates Multicast data frames dropped.
Mfdb-Cache-Hits	Shows MFDB cache hits.
Mfdb-Cache-Misses	Shows MFDB cache misses.
IGMP Statistics	
Interface	The name of the VAP interface.
Igmp-Frames	Shows IGMP frames received.
Igmp-Frames-Fwd	Shows IGMP membership queries received.
Igmp-Frames-Sentup	Shows IGMP membership reports seen.
Mfdb-Cache-Hits	Shows MFDB cache hits.
Mfdb-Cache-Misses	Shows MFDB cache misses.
Multicast-Group	
Interface	The name of the VAP interface.
Multicast-Group	Shows Multicast group IP address.
Stations	Shows Multicast group Station MAC address.
Packets	Shows Multicast group stations packets received.

4.5 «Client Associations» submenu

The associated stations are displayed along with information about packet traffic transmitted and received for each station.



View list of currently associated client stations

Click "Refresh" button to refresh the page.

Total Number of Associated Clients 1

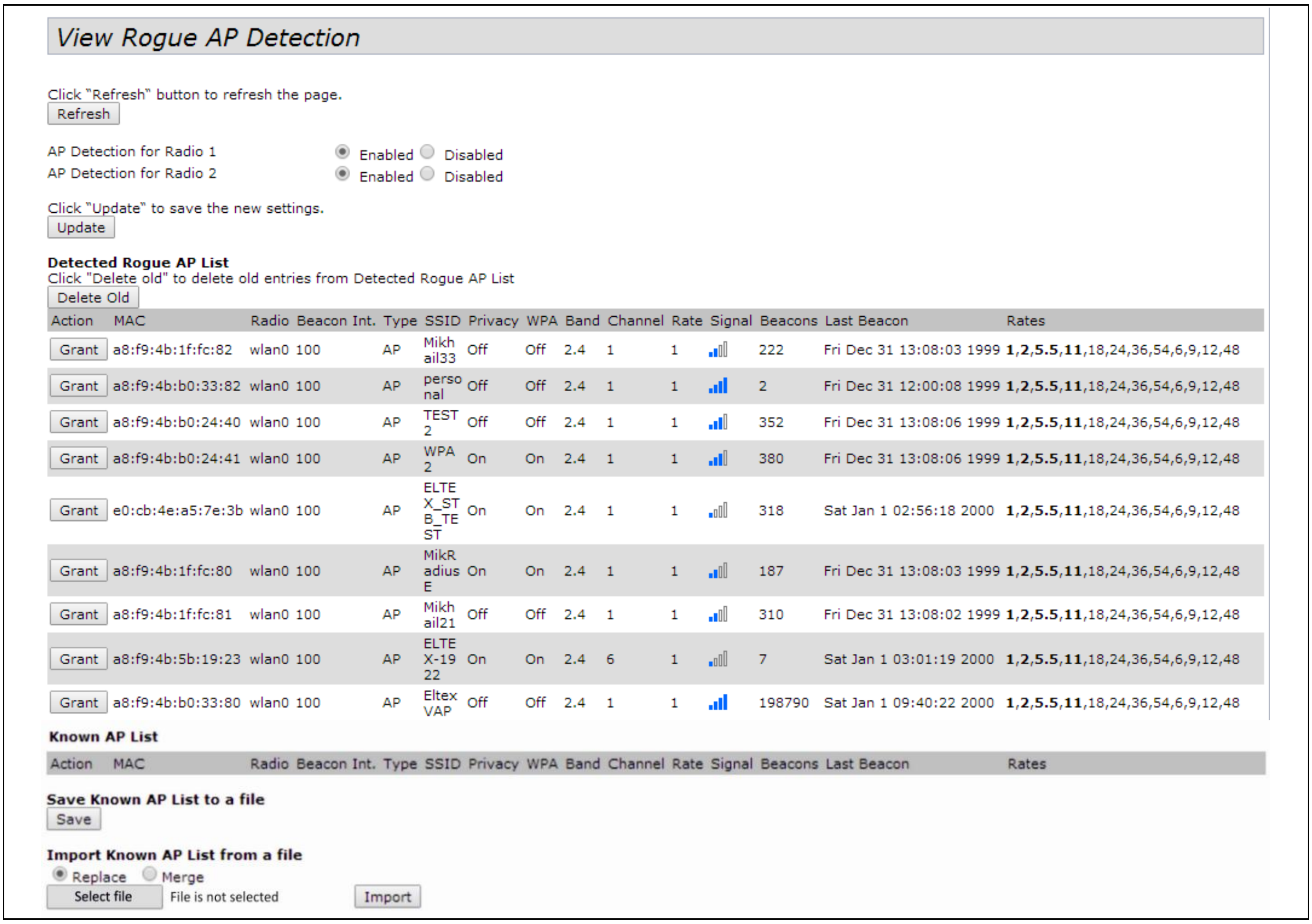
Network	Station	Status		From Station					To Station		
		Authenticated	Associated	Packets	Bytes	Drop Packets	Drop Bytes	TS Violate Pkts	Packets	Bytes	Drop Packet
wlan0	30:39:26:2b:d9:bc	Yes	Yes	591	184873	0	0		486	276402	0

Field	*Description*
Network	Shows which VAP the client is associated with. For example, an entry of wlan0vap2 means theclient is associated with Radio 1, VAP 2.An entry of wlan0 means the client is associated with VAP 0 on Radio 1. An entry of wlan1 means the client is associated with VAP 0 on Radio 2.
Station	Shows the MAC address of the associated wireless client.
Status	The Authenticated and Associated Status shows 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. Some points to keep in mind with regard to this *Field* are: • If the AP security mode is None or Static WEP, the authentication and association status ofclients showing on the Client Associations tab will be in line with what is expected; that is, if a client shows as authenticated to the AP, it will be able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.) • If the AP uses IEEE 802.1X or WPA security, however, it is possible for a client association toshow 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 These *Field*s report information about traffic sent from a wireless client to the AP.	
Packets	The number of packets received from the wireless client.
Bytes	The number of bytes received from the wireless client.
Drop Packets	The number of packets that were dropped after being received.
Drop Bytes	The number of bytes that were dropped after being received.
TS ViolatePackets	The number of packets sent from a wireless client to the AP in excess of its active TS uplinkbandwidth, or for an access category requiring admission control to which the wireless client has not been admitted.
To Station These *Field*s report information about traffic sent from the AP to a wireless client.	
Packets	The number of packets sent from the AP to the wireless client.
Bytes	The number of bytes the AP attempted to send but were dropped.
Drop Packets	The number of packets that the AP attempted to send to the wireless client but were dropped.
Drop Bytes	The number of bytes that the AP attempted to send to the wireless client but were dropped.
TS ViolatePackets	The number of packets sent from the AP to a wireless client in excess of its active TS downlinkbandwidth, or for an access category requiring admission control to which the wireless client has not been admitted.

4.6 «Rogue AP Detection» submenu

The status page for Rogue AP Detection provides real-time statistics for all APs detected by the FASTPATH UAP in the vicinity of the network.



View Rogue AP Detection

Click "Refresh" button to refresh the page.

Refresh

AP Detection for Radio 1 ● Enabled ○ Disabled

AP Detection for Radio 2 ● Enabled ○ Disabled

Click "Update" to save the new settings.

Update

Detected Rogue AP List

Click "Delete old" to delete old entries from Detected Rogue AP List

Delete Old

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Grant	a8:f9:4b:1f:fc:82	wlan0	100	AP	Mikhail33	Off	Off	2.4	1	1	▂▄	222	Fri Dec 31 13:08:03 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:b0:33:82	wlan0	100	AP	personal	Off	Off	2.4	1	1	▂▄▆█	2	Fri Dec 31 12:00:08 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:b0:24:40	wlan0	100	AP	TEST2	Off	Off	2.4	1	1	▂▄▆	352	Fri Dec 31 13:08:06 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:b0:24:41	wlan0	100	AP	WPA2	On	On	2.4	1	1	▂▄▆	380	Fri Dec 31 13:08:06 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	e0:cb:4e:a5:7e:3b	wlan0	100	AP	ELTEX_STB_TEST	On	On	2.4	1	1	▂	318	Sat Jan 1 02:56:18 2000	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:1f:fc:80	wlan0	100	AP	MikRadiusE	On	On	2.4	1	1	▂▄	187	Fri Dec 31 13:08:03 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:1f:fc:81	wlan0	100	AP	Mikhail21	Off	Off	2.4	1	1	▂▄	310	Fri Dec 31 13:08:02 1999	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:5b:19:23	wlan0	100	AP	ELTEX-1922	On	On	2.4	6	1	▂	7	Sat Jan 1 03:01:19 2000	**1,2,5.5,11**,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:b0:33:80	wlan0	100	AP	Eltex VAP	Off	Off	2.4	1	1	▂▄▆█	198790	Sat Jan 1 09:40:22 2000	**1,2,5.5,11**,18,24,36,54,6,9,12,48

Known AP List

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates

Save Known AP List to a file

Save

Import Known AP List from a file

● Replace ○ Merge

Select file File is not selected Import

Click **Update** to refresh the screen and display the most current information.

Field	*Description*
AP Detection forRadio 1	To enable Radio 1 to perform neighbor AP detection and collect information about neighbor APs, select **Enabled**. **Note:** The Spectrum Analyzer feature and Rogue AP detection feature cannot be enabled on a radio at the same time. If one feature is enabled, and you enable the other, a message displays and informs you that the other feature will be disabled. For example, if Rogue AP detection is enabled, and you enable the Dedicated Spectrum Analyzer mode, you are informed that Rogue AP detection will be disabled. To disable neighbor AP detection on Radio 1, select **Disabled**. If you change the AP detection setting, click **Update**.
AP Detection forRadio 2	To enable Radio 2 to perform neighbor AP detection and collect information about neighbor APs, select **Enabled**. **Note:** The Spectrum Analyzer feature and Rogue AP detection feature cannot be enabled on a radio at the same time. If one feature is enabled, and you enable the other, a message displays and informs you that the other feature will be disabled. For example, if Rogue AP detection is enabled, and you enable the Dedicated Spectrum Analyzer mode, you are informed that Rogue AP detection will be disabled.

	To disable neighbor AP detection on Radio 2, select **Disabled**. If you change the AP detection setting, click **Update**.
Action	The available action depends on which list an AP is in: • If the AP is in the Detected Rogue AP List, the **Grant** button is available. Click **Grant** to move the AP from the Detected Rogue AP List to the Known AP List. • If the AP is in the Known AP list, the **Delete** button is available. Click **Delete** to move the AP from the Known AP list to the Detected Rogue AP List. **Note:** The Detected Rogue AP List and Known AP List provide information. The FASTPATH UAP does not have any control over the APs on the list and cannot apply any security policies to APs detected through the RF scan.
MAC	Shows the MAC address of the neighboring AP.
Radio	The Radio *Field* indicates which radio detected the neighboring AP: • wlan0 (Radio One)wlan1 (Radio Two)
Beacon Int.	Shows 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 (or 10 per second). The Beacon Interval is set on the **Radio** page.
Type	Indicates the type of device: • **AP** indicates the neighboring device is an AP that supports the IEEE 802.11 WirelessNetworking Framework in Infrastructure Mode. • **Ad hoc** indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as *peer-to-peer*mode or an *Independent Basic Service Set* (IBSS).
SSID	The *Service Set Identifier* (SSID) for the AP. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wirelesslocal area network. It is also referred to as the *Network Name*. The SSID is set on the **VAP** page.
Privacy	Indicates whether there is any security on the neighboring device. • **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. Security is configured on the AP from the **VAP** page.
WPA	Indicates whether WPA security is on or off for this AP.
Band	This indicates the IEEE 802.11 mode being used on this AP. (For example, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.) The number shown indicates the mode according to the following map: • **2.4** indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes) • **5** indicates IEEE 802.11a or 802.11n mode (or both modes)
Channel	Shows 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 Radio Settings. **Note:** When AP is operating in DFS channel, Scanning is prohibitted, Hence No Rogue APs will be detected.
Rate	Shows the rate (in megabits per second) at which this AP is currently transmitting. The current rate will always be one of the rates shown in Supported Rates.

Signal	Indicates the strength of the radio signal emitting from this AP. If you hover the mouse pointer over the bars, a number appears and shows the strength in decibels (dB).
Beacons	Shows the total number of beacons received from this AP since it was first discovered.
Last Beacon	Shows the date and time of the last beacon received from this AP.
Rates	Shows supported and basic (advertised) rate sets for the neighboring AP. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the **Radio Settings** page.

To save the Known AP List to a file, click **Save**. The list contains the MAC addresses of all APs that have been added to the Known AP List. By default, the filename is Rogue2.cfg. You can use a text editor or Web browser to open the file and view its contents.

Use the Import feature to import a list of known APs from a saved list. The list might be from another AP or created from a text file. If the MAC address of an AP appears in the Known AP List, it will not be detected as a rogue.

To import an AP list from a file, use the following steps:

- Choose whether to replace the existing Known AP List or add the entries in the imported file to the Known AP List.

Select **Replace** to import the list and replace the contents of the Known AP List.

Select **Merge** to import the list and add the APs in the imported file to the APs currently displayed in the Known AP List.

- Click **Browse** and choose the file to import.

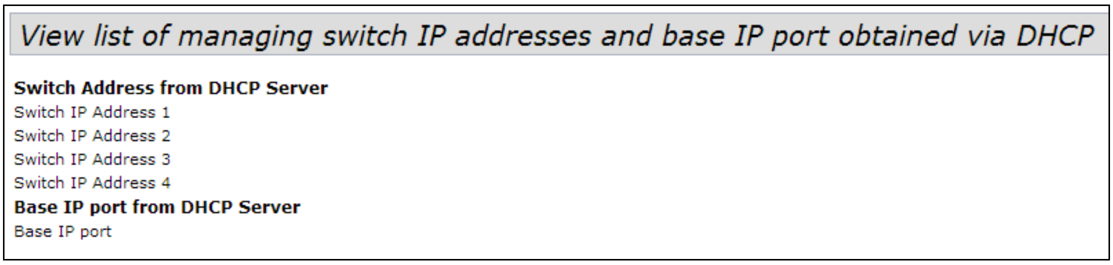
The file you import must be a plain-text file with a .txt or .cfg extension. Entries in the file are MAC addresses in hexadecimal format with each octet separated by colons, for example 00:11:22:33:44:55. Separate entries with a single space. For the AP to accept the file, it must contain only MAC addresses.

- Click **Import**.

Once the import is complete, the screen refreshes and the MAC addresses of the APs in the imported file appear in the Known AP List.

4.7 «Manage AP DHCP» submenu

The UAP can learn about FASTPATH Unified Wireless Switches on the network through DHCP responses to its initial DHCP request. The Managed AP DHCP page displays the DNS names or IP addresses of up to four FASTPATH Unified Wireless Switches and the base IP port that the AP learned about from a DHCP server on your network.



View list of managing switch IP addresses and base IP port obtained via DHCP

Switch Address from DHCP Server

Switch IP Address 1

Switch IP Address 2

Switch IP Address 3

Switch IP Address 4

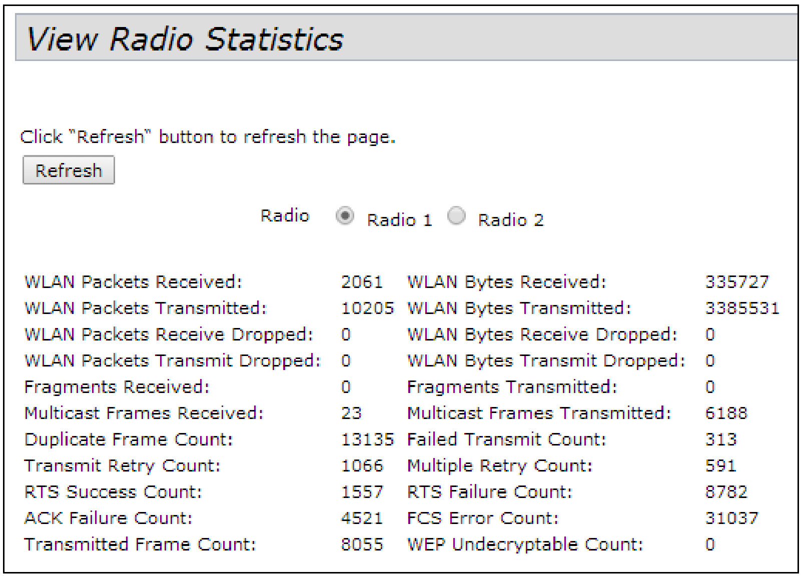
Base IP port from DHCP Server

Base IP port

- *Switch Address from DHCP Server* – The first, second, third, and fourth managing switch IP addresses retrieved through DHCP option 43;
- *Base IP port from DHCP Server* – The IP port number used for communicating with the wireless switch. The value isassigned through DHCP option 43.

4.8 «Radio Statistics» submenu

The **Radio Statistics** page show detailed information about the packets and bytes transmitted and received on the radio (wireless) interface of this access point.



View Radio Statistics

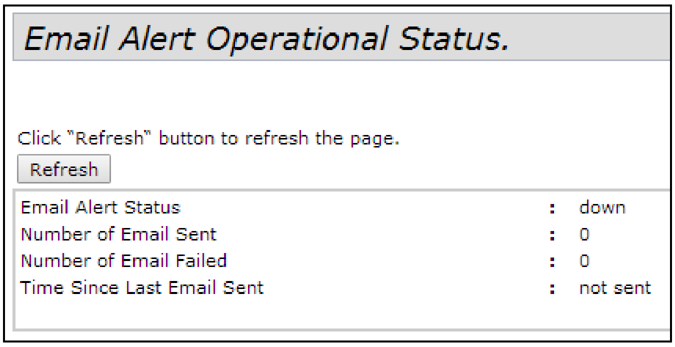
Click "Refresh" button to refresh the page.

Radio ● Radio 1 ○ Radio 2

WLAN Packets Received:	2061	WLAN Bytes Received:	335727
WLAN Packets Transmitted:	10205	WLAN Bytes Transmitted:	3385531
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:	23	Multicast Frames Transmitted:	6188
Duplicate Frame Count:	13135	Failed Transmit Count:	313
Transmit Retry Count:	1066	Multiple Retry Count:	591
RTS Success Count:	1557	RTS Failure Count:	8782
ACK Failure Count:	4521	FCS Error Count:	31037
Transmitted Frame Count:	8055	WEP Undecryptable Count:	0

4.9 «Email Alert Status» submenu

The **Email Alert Operational Status** page provides information about the email alerts sent based on the syslog messages generated in the AP.



Email Alert Operational Status.

Click "Refresh" button to refresh the page.

```
Email Alert Status              :   down
Number of Email Sent            :   0
Number of Email Failed          :   0
Time Since Last Email Sent      :   not sent
```

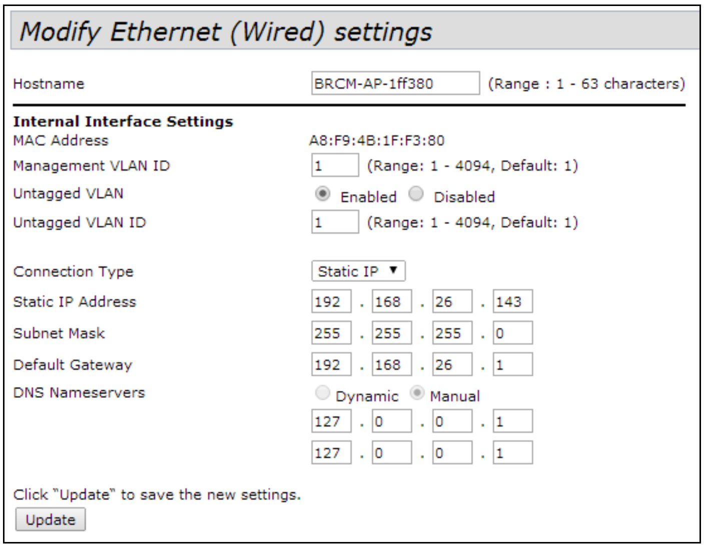
Field	***Description***
Email Alert Status	The Email Alert operational status The status is either **Up** or **Down**. The default is **Down**.
Number of Email Sent	The total number of email sent so far. The range is an unsigned integer of 32 bits. The default is 0.
Number of Email Failed	The total number of email failures so far. The range is an unsigned integer of 32 bits. The default is 0.
Time Since Last Email Sent	The time and date when the last email alert was sent. The UAP uses the system time to report the information. If an email has not been sent since the device was reset, the status is *not sent*.

5 «MANAGE» MENU

«Manage» menu provides network setting of the device.

5.1 «Ethernet Settings» submenu

The paragraph describes network setting of the.



Modify Ethernet (Wired) settings

Hostname: BRCM-AP-1ff380 (Range : 1 - 63 characters)

Internal Interface Settings

MAC Address: A8:F9:4B:1F:F3:80

Management VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Untagged VLAN: ● Enabled ○ Disabled

Untagged VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Connection Type: Static IP ▼

Static IP Address: 192 . 168 . 26 . 143

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 26 . 1

DNS Nameservers: ○ Dynamic ● Manual

127 . 0 . 0 . 1

127 . 0 . 0 . 1

Click "Update" to save the new settings.

Update

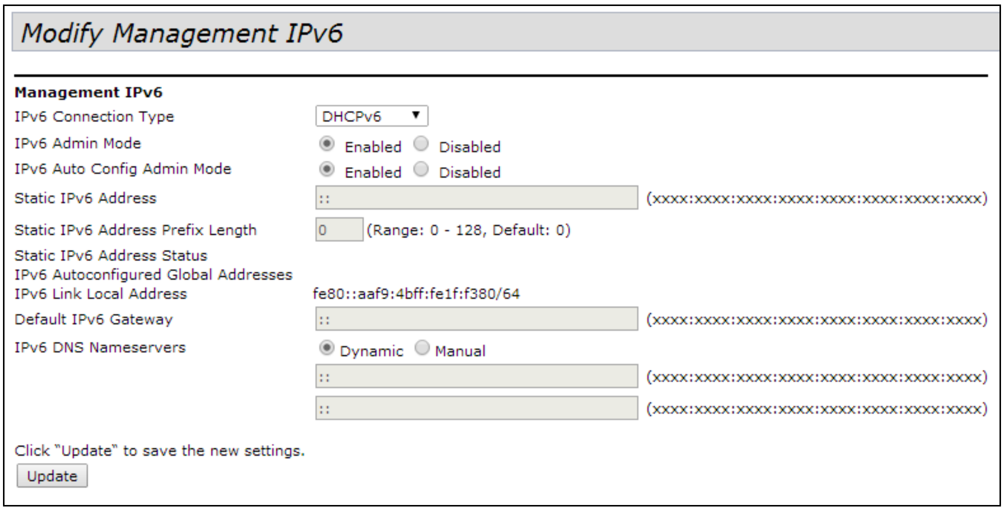
Field	Description
Hostname	Enter a hostname for the AP. The hostname appears in the CLI prompt. The hostname has the following requirements: • The length must be between 1-63 characters. • Upper and lower case characters, numbers, and hyphens are accepted; • The first character must be a letter (a-z or A-Z) or number (0-9), and the last character cannot be a hyphen.
MAC Address	Shows the MAC address for the LAN interface for the Ethernet port on this AP. This is a read-only *Field* that you cannot change.
Management VLAN ID	The management VLAN is the VLAN associated with the IP address you use to access theAP. The default management VLAN ID is 1. Provide a number between 1 and 4094 for the management VLAN ID.
Untagged VLAN	If you disable the untagged VLAN, all traffic is tagged with a VLAN ID. By default all traffic on the UAP uses VLAN 1, which is the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS.
Untagged VLAN ID	Provide a number between 1 and 4094 for the untagged VLAN ID. Traffic on the VLAN that you specify in this *Field* will not be tagged with a VLAN ID.
Connection Type	If you select **DHCP**, the UAP acquires its IP address, subnet mask, DNS, and

	gateway information from a DHCP server. If you select **Static IP**, you must enter information in the Static IP Address, Subnet Mask, and Default Gateway *Field*s.
Static IP Address	Enter the static IP address in the text boxes. This *Field* is disabled if you use DHCP as theconnection type.
Subnet Mask	Enter the **Subnet Mask** in the text boxes.
Default Gateway	Enter the **Default Gateway** in the text boxes.
DNS Nameservers	Select the mode for the DNS. In **Dynamic** mode, the IP addresses for the DNS servers are assigned automatically via DHCP. This option is only available if you specified DHCP for the Connection Type. In **Manual** mode, you must assign static IP addresses to resolve domain names.

Note: After you configure the wired settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

5.2 «Management IPv6» submenu

Management IPv6 settings describe the IPv6 configuration of Management Interface.



Modify Management IPv6

Management IPv6

IPv6 Connection Type	DHCPv6 ▼	
IPv6 Admin Mode	● Enabled ○ Disabled	
IPv6 Auto Config Admin Mode	● Enabled ○ Disabled	
Static IPv6 Address	::	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
Static IPv6 Address Prefix Length	0	(Range: 0 - 128, Default: 0)
Static IPv6 Address Status		
IPv6 Autoconfigured Global Addresses		
IPv6 Link Local Address	fe80::aaf9:4bff:fe1f:f380/64	
Default IPv6 Gateway	::	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 DNS Nameservers	● Dynamic ○ Manual	
	::	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
	::	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Click "Update" to save the new settings.

Field	***Description***
IPv6 Connection Type	If you select **DHCPv6**, the UAP acquires its IPv6 address, DNS, and gateway information from a DHCPv6 server. If you select **Static IPv6**, you must enter information in the Static IPv6 Address, Prefix length, and Default Gateway *Field*s.
IPv6 Admin Mode	Enable or disable IPv6 management access to the AP
IPv6 Auto Config Admin Mode	Enable or disable IPv6 auto address configuration on the AP. When IPv6 Auto Config Mode is enabled, automatic IPv6 address configuration and gateway configuration is allowed by processing the Router Advertisements

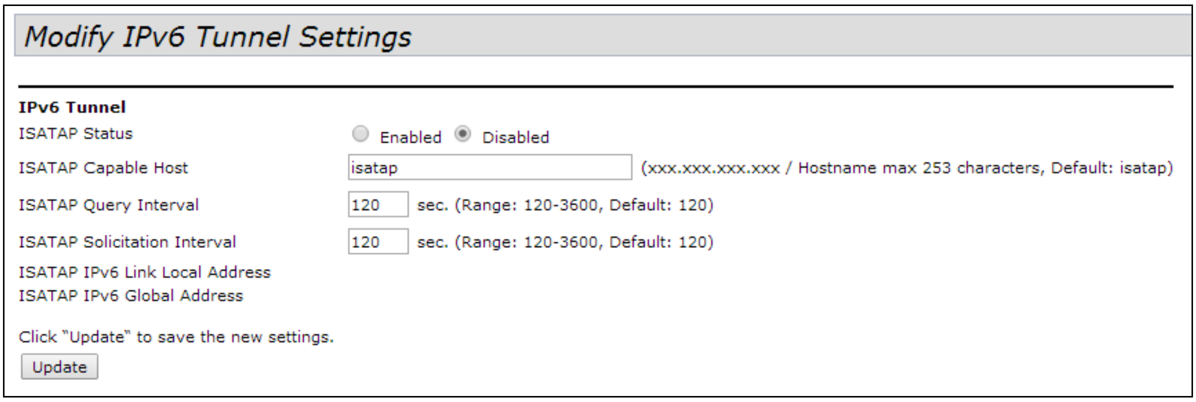
	received on the LAN port. The AP can have multiple auto configured IPv6 addresses.
Static IPv6 Address	Enter a static IPv6 address. The AP can have a static IPv6 address even if addresses have already been configured automatically.
Static IPv6 AddressPrefix Length	Enter the static IPv6 prefix length, which is an integer in the range of 0-128.
Static IPv6 AddressStatus	Shows the Static IPv6 address operational status assigned to AP's management interface.The possible values are 'Operational' and 'Tentative'.
IPv6 AutoconfiguredGlobal Addresses	If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed.
IPv6 Link Local Address	Shows the IPv6 Link Local address, which 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.
Default IPv6 Gateway	Enter the default IPv6 gateway.
IPv6 Domain Nameservers	Select the mode for the DNS. In **Dynamic** mode, the IPv6 addresses for the DNS servers are assigned automatically via DHCPv6. This option is only available if you specified DHCPv6 for the Connection Type. In **Manual** mode, you must assign static IPv6 addresses to resolve domain names.

Note: After you configure the wired settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

5.3 «IPv6 Tunnel» submenu

The ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) provides the support for encapsulating IPv6 packets within IPv4 packets to allow transmission over IPv4 networks. This feature provides AP to act as an initiator of the tunnel and will allow communication with remote IPv6 hosts. An ISATAP router acts as the end of the tunnel within the network to help AP to auto-configure ISATAP tunnel interface.

From the IPv6 Tunnel page, you can enable,configure and displays ISATAP global operational and configuration parameters.



Modify IPv6 Tunnel Settings

IPv6 Tunnel

ISATAP Status	○ Enabled ● Disabled	
ISATAP Capable Host	isatap	(xxx.xxx.xxx.xxx / Hostname max 253 characters, Default: isatap)
ISATAP Query Interval	120	sec. (Range: 120-3600, Default: 120)
ISATAP Solicitation Interval	120	sec. (Range: 120-3600, Default: 120)
ISATAP IPv6 Link Local Address		
ISATAP IPv6 Global Address		

Click "Update" to save the new settings.

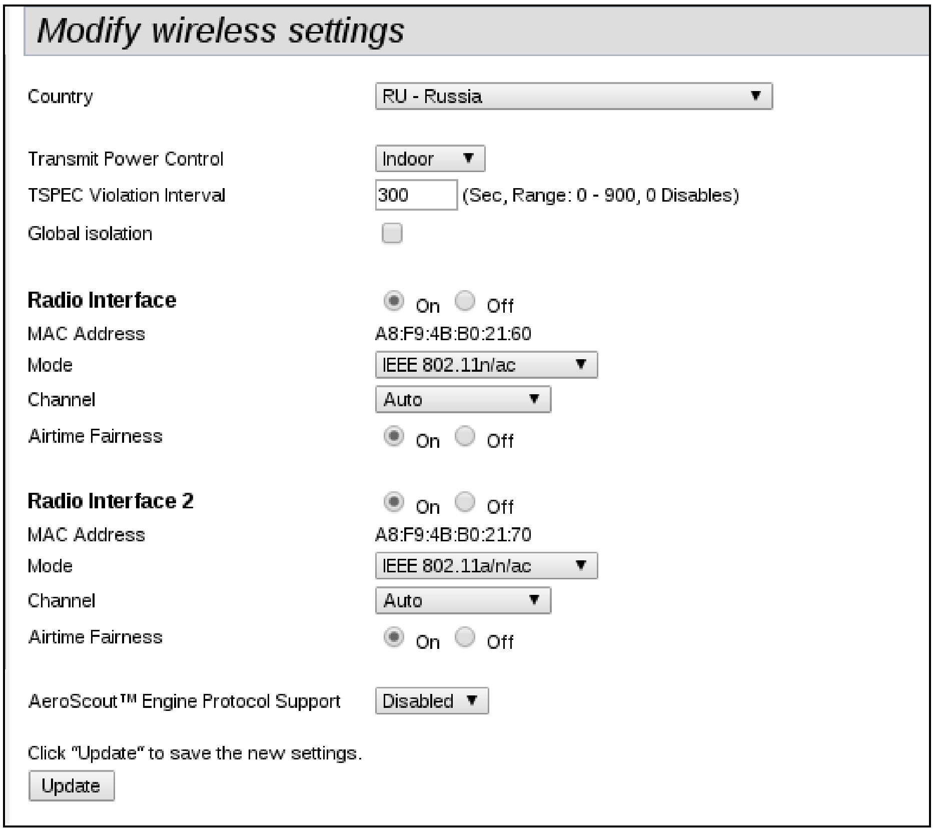
Field	***Description***
ISATAP Status	Select Enable or disable Administrative ISATAP tunnel status.
ISATAP Capable Host	Specify the IP Address or DNS name of the ISATAP router. The default value is isatap.
ISATAP Query Interval	The number of seconds from 120-3600 between DNS queries (before the IP address of the ISATAP router is known) for this tunnel. The interval can be the default value (120 seconds) or a user defined interval.
ISATAP Solicitation Interval	The number of seconds from 120-3600 between ISATAP router solicitations messages, when there is no active ISATAP router. The interval can be the default value (120 seconds) or a user defined interval.
ISATAP IPv6 Link Local Address	Displays link-local IPv6 address of ISATAP interface.
ISATAP IPv6 Global Address	Displays global IPv6 address of ISATAP interface.

Note: To apply your changes, click **Update**. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

5.4 «Wireless Settings» submenu

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID).

Note: Radio interface settings apply to both Radio Interface One and Radio Interface Two.



Modify wireless settings

Country: RU - Russia

Transmit Power Control: Indoor

TSPEC Violation Interval: 300 (Sec, Range: 0 - 900, 0 Disables)

Global isolation: □

Radio Interface ● On ○ Off

MAC Address: A8:F9:4B:B0:21:60

Mode: IEEE 802.11n/ac

Channel: Auto

Airtime Fairness: ● On ○ Off

Radio Interface 2 ● On ○ Off

MAC Address: A8:F9:4B:B0:21:70

Mode: IEEE 802.11a/n/ac

Channel: Auto

Airtime Fairness: ● On ○ Off

AeroScout™ Engine Protocol Support: Disabled

Click "Update" to save the new settings.

Field	*Description*
Country	Select the country in which the AP is operating. Wireless regulations vary from country to country. Make sure you select the correct country code so that the AP complies with the regulations in your country. The country code selection affects the radio modes the AP can support as well as the list of channels and transmission power of the radio.
Transmit Power Control	Transmit Power Control – restraint mode configuration of *Transmit Power Limit* parameter: • **Indoor** –EIRP maximum value must be no more than 100 mW (16 dBm transmitter radiated power for 2,4 MHz and 19 dBm transmitter radiated power for 5 MHz) in accordance with Russian Federation regulation. • **Outdoor** - EIRP maximum value is limited by physical characteristics of a transmitter.
TSPEC Violation Interval	Specify the time interval (in seconds) for the AP to report (through the system log and SNMP traps) associated clients that do not adhere to mandatory admission control procedures.
Global isolation	Enables the isolation between clients in different VAP and different Radio.
Radio Interface	Specify whether you want the radio interface on or off.
MAC Address	Indicates the Media Access Control (MAC) addresses for the interface. This page shows the MAC addresses for Radio Interface One and Radio Interface Two. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.
Mode	The **Mode** defines the Physical Layer (PHY) standard the radio uses **Note:** The modes available depend on the country code setting. Select one of the following modes for each radio interface:
Channel	Select the **Channel**. The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected. 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). When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel *Field*. This allows the automatic channel feature to set the channels for the radios in the cluster.
AeroScout™ Engine Protocol Support	Options are **Enabled** or **Disabled**. The default is **Disabled**. When enabled, Aerosc out devices are recognized and data is sent to an Aeroscout Engine (AE) for analysis. The AE determines the geographical location of 802.11-capable devices, such as STAs, APs, and AeroScout's line of 802.11-enabled RFID devices, or *tags*. The AE communicates with APs that support the AE protocol in order to collect information about the RF devices detected by the APs. Using the AE protocol, FASTPATH supports direct communication between AE and the APs. When operating in managed mode, the AE is configured with the IP address of the managed access points from which it collects information. The Wireless Switch cannot communicate with the AE. **Note:** Only AeroScout tag hardware of types T2 and T3 are explicitly supported.

	Other tag models are also supported only if their implementation of the AeroScout protocol conforms to the *AeroScout Engine - Access Point Interface Specification.* **Note:** AeroScout tags operate only in 802.11 b/g mode. Therefore, network administrators who use the AeroScout tags must configure at least one radio on APs that are expected to detect tags in either 802.11b/g or 802.11b/g/n mode. The radios configured in 2.4 GHz IEEE 802.11 mode or any of the 5 GHZ modes cannot detect AeroScout tags. **Note:** The AE protocol allows access points to mark detected APs as rogue devices. The FASTPATH APs do not support this feature and never report detected APs as rogues.

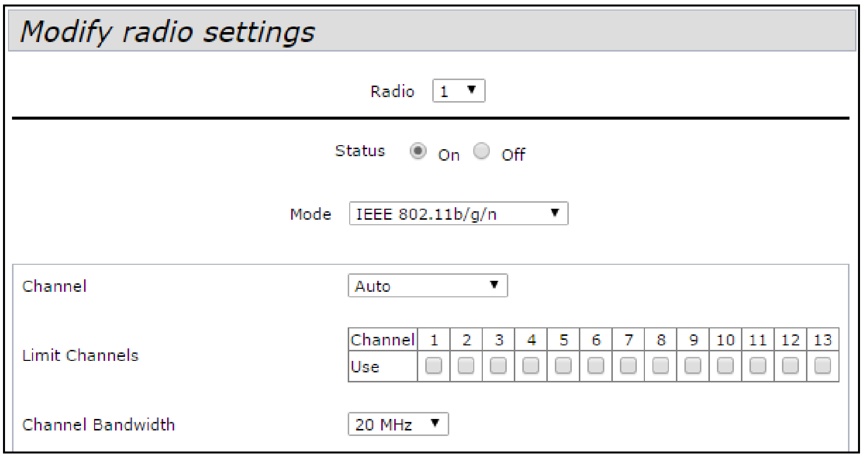
Note: After you configure the wireless settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Click **Update** to save the new settings.

5.5 «Radio» submenu

Radio settings directly control the behavior of the radio devices in the AP and its interaction with the physical medium; that is, how and what type of electromagnetic waves the AP emits.

Different settings display depending on the mode you select. All settings are described in the following table.



Modify radio settings

Radio 1

Status ● On ○ Off

Mode IEEE 802.11b/g/n

Channel Auto

Limit Channels

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Use	□	□	□	□	□	□	□	□	□	□	□	□	□

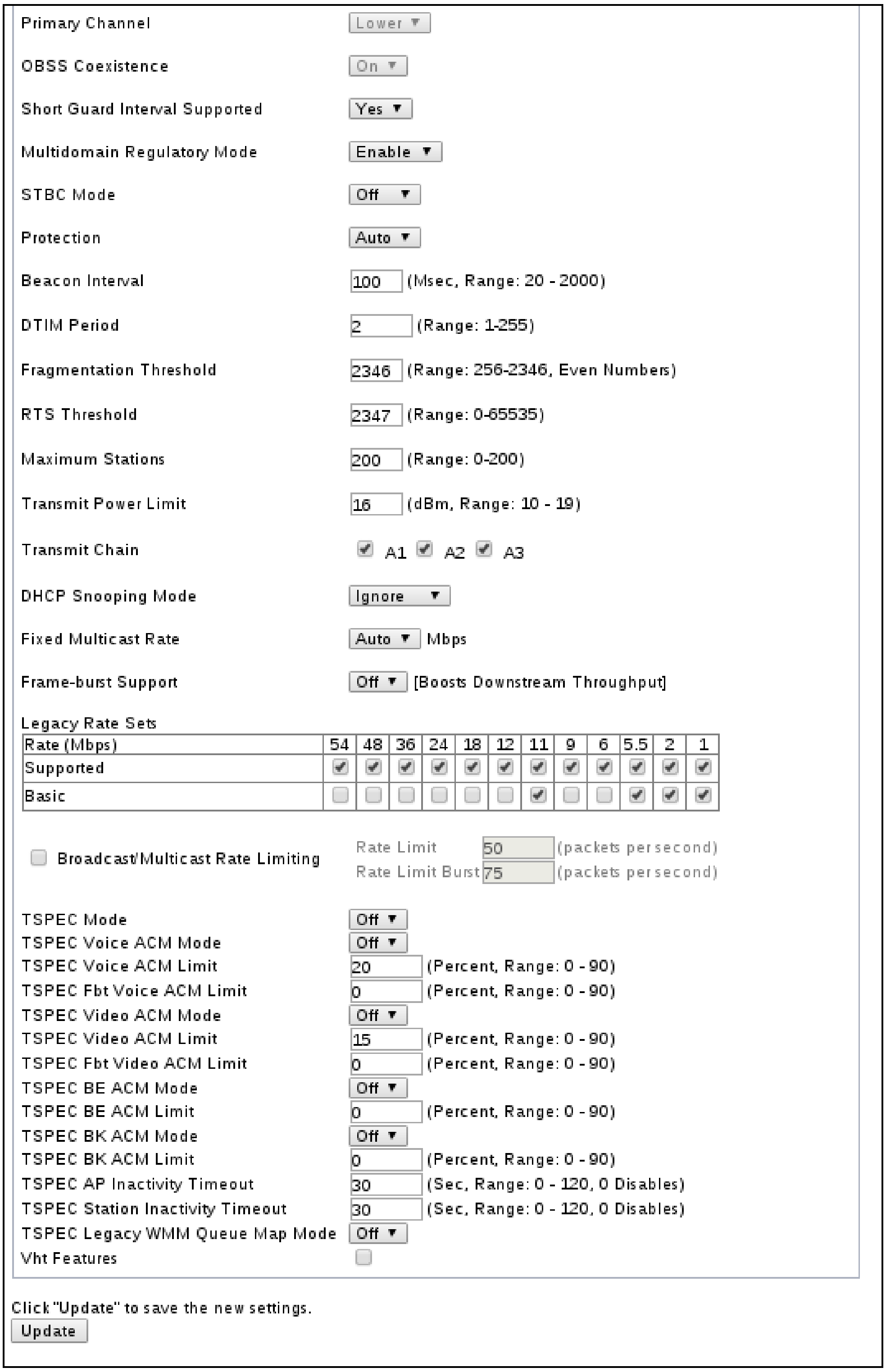
Channel Bandwidth 20 MHz

Field	***Description***
Radio	Select Radio 1or Radio 2 to specify which radio to configure. The rest of the settings on this tab apply to the radio you select in this *Field*. Be sure to configure settings for both radios.
Status (On/Off)	Specify whether you want the radio on or off by clicking **On** or **Off**. If you turn off a radio, the AP sends disassociation frames to all the wireless clients it iscurrently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.
Mode	The **Mode** defines the Physical Layer (PHY) standard the radio uses **Note:** The modes available depend on the country code setting and radio. Select one of the following modes for each radio interface: • IEEE 802.11b/g-802.11b and 802.11g clients can connect to the AP. • IEEE 802.11b/g/n -802.11b, 802.11g, and 802.11n clients operating in

	the 2.4-GHz frequency can connect to the AP. • 2.4 GHz IEEE 802.11n-Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP. • IEEE 802.11a -Only 802.11a clients can connect to the AP. • IEEE 802.11a/n-802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 1. • 5 GHz IEEE 802.11n-Only 802.11n clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 1. • IEEE 802.11a/n/ac-802.11a, 802.11n, and 802.11ac clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 2. • IEEE 802.11n/ac-802.11n clients and 802.11ac clients operating in the 5-GHz frequency can connect to the AP. This mode is available only on Radio 2.
Channel	Select the **Channel**. The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the AP scans available channels and selects a channel where no traffic is detected. 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). When automatic channel assignment is enabled on the Channel Management page for Clustering, the channel policy for the radio is automatically set to static mode, and the Auto option is not available for the Channel *Field*. This allows the automatic channel feature to set the channels for the radios in the cluster.
Limit Channels	Limit Channels allows you to specify a list of channels that will be available to automatically selection. To configure this feature if the value of the Channel Bandwidth over 20 MHz, you must specify several adjacent channels, to the total bandwidth matches the value of Channel Bandwidth.
Channel Bandwidth(802.11n and 802.11ac modes only)	The 802.11n specification allows a 40 MHz-wide channel in addition to the legacy 20 MHz channel available with other modes. The 40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 802.11ac specification allows an 80 MHz-wide channel in addition to the 20 MHz and 40 MHz channels. Set the *Field* to 20 MHz to restrict the use of the channel bandwidth to a 20 MHz channel. For the 802.11ac mode, set the *Field* to 40 MHz to prevent the radio from using the 80 MHz channel bandwidth.

Wi-Fi client devices may not support some frequency channels. 1-11 frequency channals are recommended to set for 2.4 GHz range and 36-48 for 5GHz range if no information about channels supported by clients.

When you set frequency channel from 52-144 range, Wi-Fi interface will be connected after minute.



Primary Channel	Lower ▼
OBSS Coexistence	On ▼
Short Guard Interval Supported	Yes ▼
Multidomain Regulatory Mode	Enable ▼
STBC Mode	Off ▼
Protection	Auto ▼
Beacon Interval	100 (Msec, Range: 20 - 2000)
DTIM Period	2 (Range: 1-255)
Fragmentation Threshold	2346 (Range: 256-2346, Even Numbers)
RTS Threshold	2347 (Range: 0-65535)
Maximum Stations	200 (Range: 0-200)
Transmit Power Limit	16 (dBm, Range: 10 - 19)
Transmit Chain	☑ A1 ☑ A2 ☑ A3
DHCP Snooping Mode	Ignore ▼
Fixed Multicast Rate	Auto ▼ Mbps
Frame-burst Support	Off ▼ [Boosts Downstream Throughput]

Legacy Rate Sets

Rate (Mbps)	54	48	36	24	18	12	11	9	6	5.5	2	1
Supported	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Basic	□	□	□	□	□	□	☑	□	□	☑	☑	☑

□ Broadcast/Multicast Rate Limiting	Rate Limit	50 (packets per second)
	Rate Limit Burst	75 (packets per second)

TSPEC Mode	Off ▼
TSPEC Voice ACM Mode	Off ▼
TSPEC Voice ACM Limit	20 (Percent, Range: 0 - 90)
TSPEC Fbt Voice ACM Limit	0 (Percent, Range: 0 - 90)
TSPEC Video ACM Mode	Off ▼
TSPEC Video ACM Limit	15 (Percent, Range: 0 - 90)
TSPEC Fbt Video ACM Limit	0 (Percent, Range: 0 - 90)
TSPEC BE ACM Mode	Off ▼
TSPEC BE ACM Limit	0 (Percent, Range: 0 - 90)
TSPEC BK ACM Mode	Off ▼
TSPEC BK ACM Limit	0 (Percent, Range: 0 - 90)
TSPEC AP Inactivity Timeout	30 (Sec, Range: 0 - 120, 0 Disables)
TSPEC Station Inactivity Timeout	30 (Sec, Range: 0 - 120, 0 Disables)
TSPEC Legacy WMM Queue Map Mode	Off ▼
Vht Features	□

Click "Update" to save the new settings.

Field	*Description*
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**-Set the Primary Channel as the upper 20-MHz channel in the 40-MHz band. • **Lower**-Set the Primary Channel as the lower 20-MHz channel in the 40-MHz

	band.
DFS Support	This *Field* is available only if the selected radio mode operates in the 5 GHz frequency. For radios in the 5 GHz band, when DFS support is on and the regulatory domain requires radar detection on the channel, the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features of 802.11h are activated. DFS is a mechanism that requires wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP.
Short Guard Interval Supported	This *Field* is available only if the selected radio mode includes 802.11n. The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput. Select one of the following options: • Yes-The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the short guard unterval. • No-The AP transmits data using an 800 ns guard interval.
MultidomainRegulatory Mode	This feature is configurable on a per radio basis. By default it is enabled. Multidomain Regulatory Mode (World Mode) causes the AP to broadcast which country it is operating in as a part of its beacons and probe responses. This allows client stations to operate in any country without reconfiguration. Disabling this feature prevents the country code setting from being broadcast in the beacons. However, this only applies to radios configured to operate in the *g* band (2.4 GHz band). For radios operating in the *a* band (5 GHz band), the AP software configures support for 802.11h. When 802.11h is supported, the country code information is broadcast in the beacons. To enable Multidomain Regulatory Mode support, click **Enabled**. To disable Multidomain Regulatory Mode support, click **Disabled**.
STBC Mode	This *Field* is available only if the selected radio mode includes 802.11n. Space Time Block Coding (STBC) is an 802.11n technique intended to improve there liability 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. Select one of the following options: • On-The AP transmits the same data stream on multiple antennas at the same time. • Off-The AP does not transmits the same data on multiple antennas.
Protection	The protection feature contains rules to guarantee that 802.11 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 (**Off**) these protection mechanisms; however, when protection is off, 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 (or 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 client stations, currently sleeping in low-power mode,

	have data buffered on the AP awaiting pick-up. 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 between 256 and 2,346 to set the frame size threshold in bytes. The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold you set, the fragmentation function is activated and the packet is sent as multiple 802.11 frames. If the packet 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 plays no role when Aggregation is enabled. Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because 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. We recommend 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 between 0 and 65535. 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 a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Maximum Stations	Specify the maximum number of stations allowed to access this AP at any one time. You can enter a value between 0 and 200.
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 increase 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	Select the multicast traffic transmission rate you want the AP to support.
Frame-burst Support	Frame-burst Support boosts up the downstream throughput.
Legacy Rate Sets	Check the transmission rate sets you want the AP to support and the basic rate sets you want the AP to advertise: **Rates** are expressed in megabits per second. **Supported Rate Sets** indicate rates that the AP supports. You can check multiple rates (click a check box to select or de-select a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. **Basic Rate Sets** indicate rates that the AP will advertise to the network for the

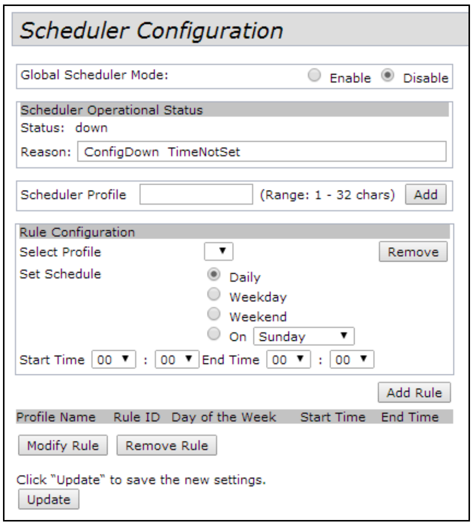
	purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.
MCS (Data Rate)Settings (802 .11n modes only)	Select the Modulation and Coding Scheme (MCS) index values for the radio should advertise to 802.11n wireless clients. The MCS indexes (also known as MCS data rates) are defined in the 802.11n specification.
Broadcast/Multicast Rate Limiting	Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. By default the **Multicast/Broadcast Rate Limiting** option is disabled. Until you enable **Multicast/Broadcast Rate Limiting**, the following *Field*s will be disabled.
Broadcast/Multicast 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.
Broadcast/Multicast Rate Limit Burst	Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit. The default and maximum rate limit burst setting is 75 packets per second.
TSPEC Mode	Regulates the overall TSPEC mode on the AP. The options are: • **On**-The AP handles TSPEC requests according to the TSPEC settings you configure on the **Radio** page. Use this setting if the AP handles traffic from QoS-capable devices, such as a Wi-Fi CERTIFIED phone. • **Off**-The AP ignores TSPEC requests from client stations. Use this setting if you do not want to use TSPEC to give QoS-capable devices priority for time-sensitive traffic.
TSPEC Voice ACMMode	Regulates mandatory admission control (ACM) for the voice access category. The options are: • **On**-A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a voice traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted. • **Off**-A station can send and receive voice priority traffic without requiring an admitted TSPEC; the AP ignores voice TSPEC requests from client stations.
TSPEC Voice ACMLimit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a voice AC to gain access.
TSPEC Fbt Voice ACMLimit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a voice AC for stations roamed to this AP using Fast BSS Transition.
TSPEC Video ACMMode	Regulates mandatory admission control for the video access category. The options are: • **On**-A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a video traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted. • **Off**-A station can send and receive video priority traffic without requiring an admitted TSPEC; the AP ignores video TSPEC requests from client stations.
TSPEC Video ACMLimit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a video AC to gain access.
TSPEC Fbt Video ACMLimit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a video AC for stations roamed to this AP using Fast BSS Transition.
TSPEC BE ACM Mode	Regulates mandatory admission control for the best effort access category. The options are: • **On**-A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a best effort traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.

	- **Off**-A station can send and receive best effort priority traffic without requiring an admitted TSPEC; the AP ignores best effort TSPEC requests from client stations.
TSPEC BE ACM Limit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a best effort AC for stations roamed to this AP using Fast BSS Transition.
TSPEC BK ACM Mode	Regulates mandatory admission control for the background access category. The options are: - **On**-A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a background traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted. - **Off**-A station can send and receive background priority traffic without requiring an admitted TSPEC; the AP ignores background TSPEC requests from client stations.
TSPEC BK ACM Limit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a background AC for stations roamed to this AP using Fast BSS Transition.
TSPEC Fbt Video ACMLimit	Specify an upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a video AC for stations roamed to this AP using Fast BSS Transition.
TSPEC AP InactivityTimeout	Specify the amount of time for an AP to detect an downlink TS as idle before deleting it.
TSPEC StationInactivity Timeout	Specify the amount of time for an AP to detect an uplink TS as idle before deleting it.
TSPEC Legacy WMMQueue Map Mode	Select **On** to allow intermixing of legacy traffic on queues operating as ACM.
Vht Features	The purpose of this feature is to enable/disable Broadcom specific extensions in VHT for Broadcom-to-Broadcom links. VHT feature enables support for 256QAM VHT rates not specified by the 802.11ac Draft. The rates are all VHT LDPC mode, MCS 9 Nss 1 20Mhz, MCS 9 Nss 2 20Mhz, MCS 6 Nss 3 80Mhz. The vht feature is supported for 802.11ac phy.

Click **Update** to save the new settings.

5.6 «Scheduler» submenu

The Radio and VAP scheduler is a standalone FASTPATH UAP feature. The Radio and VAP Scheduler allows you to configure a rule with a specific time interval for VAPs or radios to be operational, thereby automating the enabling or disabling of the VAPs and Radios.



Scheduler Configuration

Global Scheduler Mode: ○ Enable ● Disable

Scheduler Operational Status

Status: down

Reason: ConfigDown TimeNotSet

Scheduler Profile (Range: 1 - 32 chars) Add

Rule Configuration

Select Profile Remove

Set Schedule ● Daily ○ Weekday ○ Weekend ○ On Sunday

Start Time 00 : 00 End Time 00 : 00

Add Rule

Profile Name Rule ID Day of the Week Start Time End Time

Modify Rule Remove Rule

Click "Update" to save the new settings.

Update

Field	***Description***
Global Scheduler Mode	A global switch to enable or disable the scheduler feature. The default is **Disable**.
Scheduler Operational Status	
Status	The operational status of the Scheduler. The range is Up or Down. The default is **Down**.
Reason	Provides additional information about the status. The reason can be one or more of the following: • IsActive – Operational status is up. • ConfigDown – Operational status is down because global configuration is disabled. • TimeNotSet – Operational status is down because the AP time has not been set, either manually or by specifying an NTP server to use. • ManagedMode– Operational status is down because the AP is in managed mode.
Scheduler Profile	The Scheduler profile defines the list of profiles names that can be associated to the VAP or Radio configuration. Rules are associated with a named scheduler profile. You can define up to 16 scheduler profile names. By default, no profiles are created. The profile name can be up to 32 alphanumeric characters. Click **Add** to add the profile name.
Rule Configuration	Each scheduler profile may have up to 16 periodic rules. This table includes the settings you use to configure periodic rules.
Select Profile	Select the profile name from the menu.
Set Schedule	The day of the week. Range is: **Daily**, **Weekday** (Monday to Friday), **Weekend** (Saturday and Sunday),**Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**. The default is **Daily**.
Start Time	The time when the radio or VAP will be operationally enabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
End Time	The time when the radio or VAP will be operationally disabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

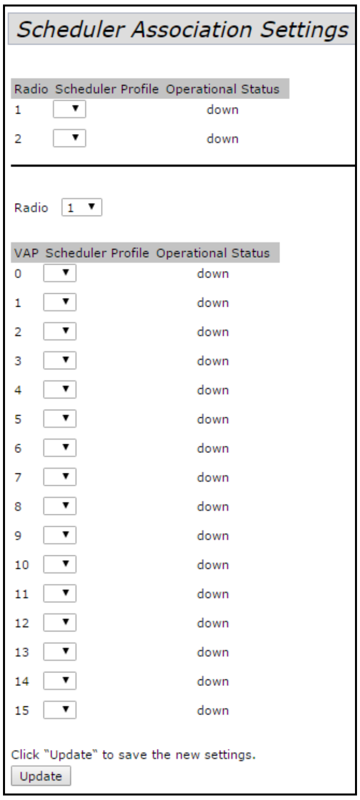
After you select a profile from the **Select Profile** *Field*, the rules that have been added to the selected profile appear in the table below the Rule Configuration area. When you add a new rule to a profile, it appears in the table. Use the **Modify Rule** and **Remove Rule** buttons to manage the rules associated with a profile.
Use the buttons to perform the following tasks:

- **Add**: To add a scheduler profile, specify the name of the profile in the appropriate *Field* and click **Add**.
- **Remove**: To remove a scheduler profile, select it from the Select Profile *Field* in the Rule Configuration table and click **Remove**.
- **Add Rule**: After you configure the rule settings, click **Add Rule** to add the rule to the selected profile.
- **Modify Rule**: To change an existing rule, select the rule, update the values in the Rule Configuration area, and click **Modify Rule**.
- **Remove Rule**: To delete a rule from a profile, select the rule and click **Remove Rule.**
- **Update**: After making any modifications to the rules, click **Update** to apply the changes and to save the settings.

5.7 «Scheduler Association» submenu

For a Scheduler profile to take effect, you must associate it with at least one radio or VAP interface. By default, there are no Scheduler profiles created, so no profile is associated to any radio or VAP. The Scheduler profile needs to be explicitly associated to a radio or VAP configuration. Only one Scheduler profile can be associated to any radio or VAP configuration; however, a single profile can be associated to multiple radios or VAPs. If the Scheduler profile associated with a VAP or radio is deleted, then the associated profile to the VAP or radio is removed implicitly. If the radio is operationally disabled, then all the VAPs associated to that radio are also operationally disabled irrespective of the VAP configuration.

The Scheduler profiles need to be associated to a Radio interface or the VAP interface for applying the periodic rules to a specific radio or VAP.



Scheduler Association Settings

Radio	Scheduler Profile	Operational Status
1	▼	down
2	▼	down

Radio 1 ▼

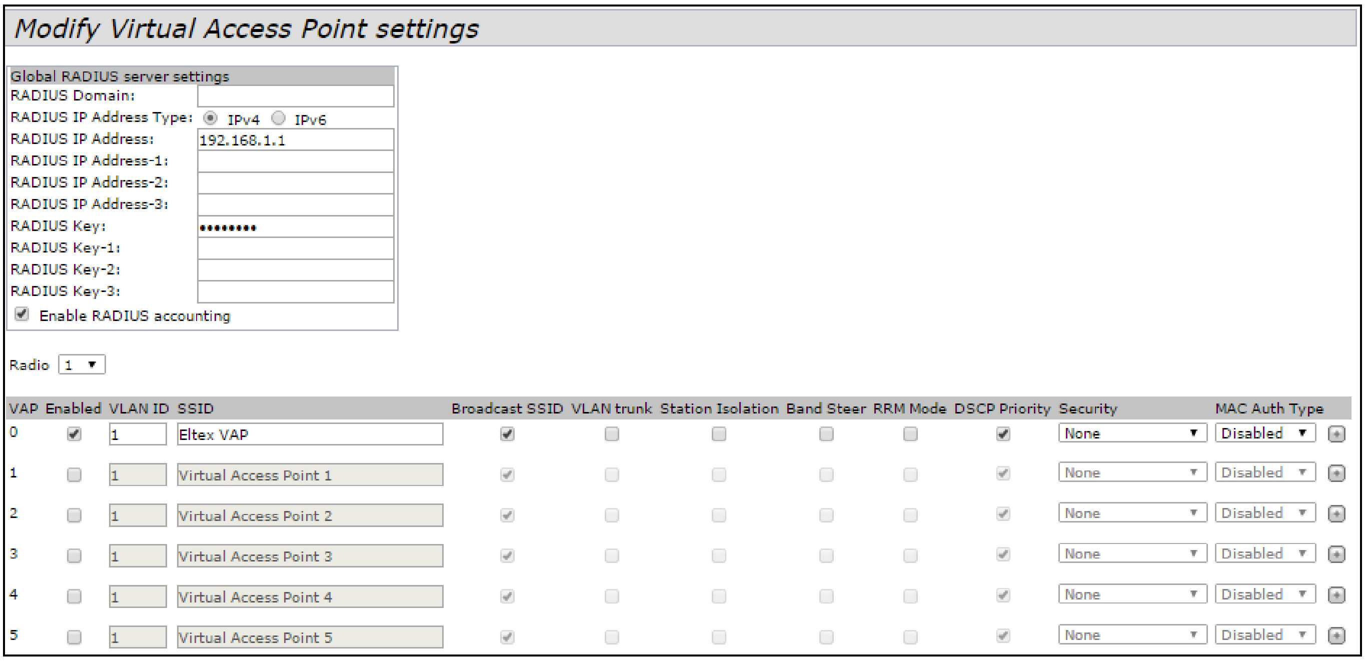
VAP	Scheduler Profile	Operational Status
0	▼	down
1	▼	down
2	▼	down
3	▼	down
4	▼	down
5	▼	down
6	▼	down
7	▼	down
8	▼	down
9	▼	down
10	▼	down
11	▼	down
12	▼	down
13	▼	down
14	▼	down
15	▼	down

Click "Update" to save the new settings.

Click **Update** to save the new settings.

5.8 «VAP» submenu

Virtual Access Points (VAPs) segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple APs in one physical AP. Each radio supports up to 16 VAPs.



Modify Virtual Access Point settings

Global RADIUS server settings

RADIUS Domain:	
RADIUS IP Address Type:	● IPv4 ○ IPv6
RADIUS IP Address:	192.168.1.1
RADIUS IP Address-1:	
RADIUS IP Address-2:	
RADIUS IP Address-3:	
RADIUS Key:	••••••••
RADIUS Key-1:	
RADIUS Key-2:	
RADIUS Key-3:	

☑ Enable RADIUS accounting

Radio 1

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	VLAN trunk	Station Isolation	Band Steer	RRM Mode	DSCP Priority	Security	MAC Auth Type
0	☑	1	Eltex VAP	☑	□	□	□	□	☑	None	Disabled
1	□	1	Virtual Access Point 1	☑	□	□	□	□	☑	None	Disabled
2	□	1	Virtual Access Point 2	☑	□	□	□	□	☑	None	Disabled
3	□	1	Virtual Access Point 3	☑	□	□	□	□	☑	None	Disabled
4	□	1	Virtual Access Point 4	☑	□	□	□	□	☑	None	Disabled
5	□	1	Virtual Access Point 5	☑	□	□	□	□	☑	None	Disabled

Global RADIUS server settings

Field	*Description*
RADIUS IP AddressType	Specify the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the AP contacts only the RADIUS server or servers for the address type you select in this *Field*.
RADIUS IP Address ***RADIUS IPv6 Address***	Enter the IPv4 or IPv6 address for the primary global RADIUS server. By default, each VAP uses the global RADIUS settings that you define for the AP at the top of the **VAP** page. When the first wireless client tries to authenticate with the AP, the AP sends an authentication request to the primary server. If the primary server responds to the authentication request, the AP continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify. If the IPv4 RADIUS IP Address Type option is selected in the previous *Field*, enter the IP address of the RADIUS server that all VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.
RADIUS IP or IPv6 Address 1-3	Enter up to three IPv4 or IPv6 addresses to use as the backup RADIUS servers. The *Field* label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected. If authentication fails with the primary server, each configured backup server is tried in sequence. The IPv4 or IPv6 address must be valid in order for the AP to attempt to contact the server.
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 1-3	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.

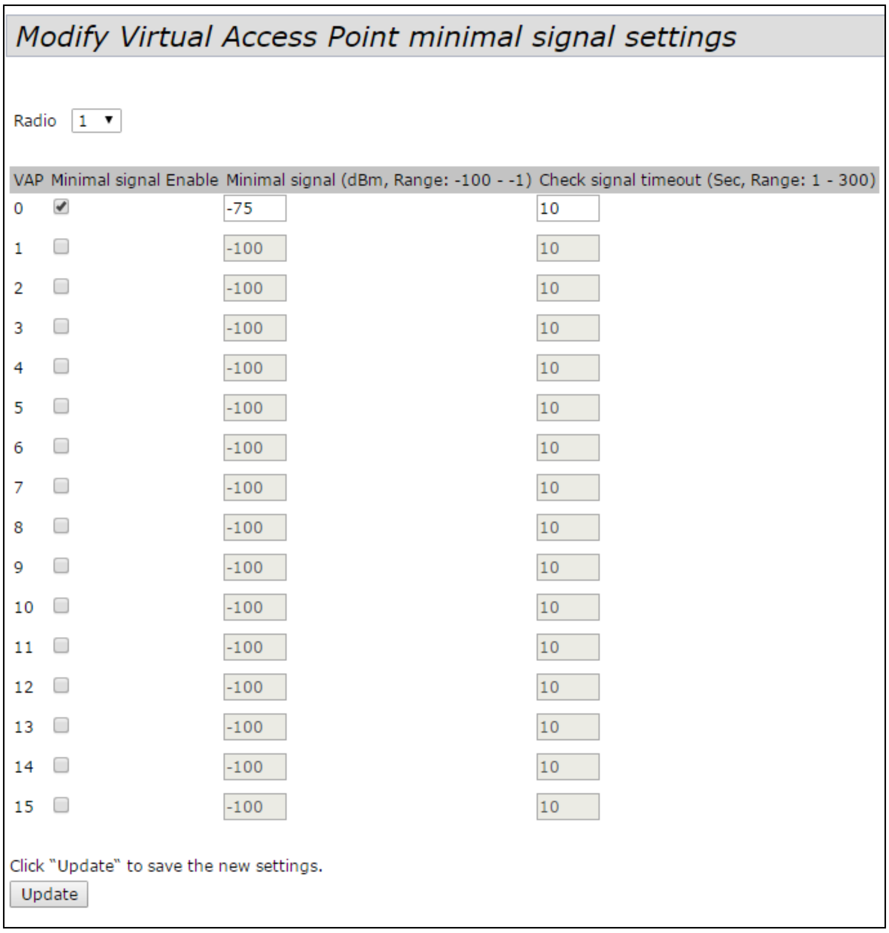
Field	***Description***
Radio	Select the radio to configure. VAPs are configured independently on each radio.
VAP	You can configure up to 16 VAPs for each radio. VAP0 is the physical radio interface, so to disable VAP0, you must disable the radio.
Enabled	You can enable or disable a configured network. If you disable the specified network, you will lose the VLAN ID you entered.
VLAN ID	When a wireless client connects to the AP by using this VAP, the AP tags all traffic from the wireless client with the VLAN ID you enter in this *Field* unless you enter the untagged VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is 1-4094. If you use RADIUS-based authentication for clients, you can optionally add the following attributes to the appropriate file in the RADIUS or AAA server to configure a VLAN for the client: The RADIUS-assigned VLAN ID overrides the VLAN ID you configure on the **VAP** page. You configure the untagged and management VLAN IDs on the **Ethernet Settings** page.
SSID	Enter a name for the wireless network. The SSID is a string of up to 32 characters. You can use the same SSID for multiple VAPs, or you can choose a unique SSID for each VAP. **Note:** If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.
Broadcast SSID	Specify whether to allow the AP to broadcast the Service Set Identifier (SSID) in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect. **Note:** Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.
Band Steer	You can enable or disable a band steer mode.
RRM Mode	Enables Radio Resource Measurement mode. Enabling RRM mode advertises RRM Capability Information element in Beacons with link measurement, Neighbor Report, Beacon Active, Beacon Passive and Beacon Table capabilities.
DSCP Priority	If you enable DSCP Priority, it will be used for prioritization, else 802.11p will be

	used.
Security	Select one of the following **Security** modes for this VAP: If you select a security mode other than None, additional *Field*s appear. These *Field*s are explained below. **Note:** The security mode you set here is specifically for this VAP.
MAC Authentication Type	You can configure a global list of MAC addresses that are allowed or denied access to the network. The drop-down menu for this feature allows you to select the type of MAC Authentication to use:
MFP (Management Frame Protection)	Provides security for the otherwise unprotected and unencrypted 802.11 management frames. This *Field* is visible only when wpa2 security and CCMP *Field*s are enabled. Following 3 check box values can be configured for it. • Not Required; • Capable; • Required. By default Capable is selected. On selecting Required, Capable checkbox will be selected and disabled.

Note: After you configure the VAP settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

5.9 «VAP Minimal Signal» submenu

Submenu provides settings of the switching off option for the Wi-Fi client equipment when the level of the signal received from it is low.



Modify Virtual Access Point minimal signal settings

Radio 1 ▾

VAP	Minimal signal Enable	Minimal signal (dBm, Range: -100 - -1)	Check signal timeout (Sec, Range: 1 - 300)
0	☑	-75	10
1	☐	-100	10
2	☐	-100	10
3	☐	-100	10
4	☐	-100	10
5	☐	-100	10
6	☐	-100	10
7	☐	-100	10
8	☐	-100	10
9	☐	-100	10
10	☐	-100	10
11	☐	-100	10
12	☐	-100	10
13	☐	-100	10
14	☐	-100	10
15	☐	-100	10

Click "Update" to save the new settings.

Field	***Description***
Minimal signal Enable	By default the Minimal signal Enable option is disabled. Until you enable Minimal signal Enable, the following *Field*s will be disabled.
Minimal signal	Enter the minimal signal level. The level should greater than or equal to -100, but less than or equal to -1 dBm.
Check signal timeout	Enter check signal timeout. The timeout should be greater than or equal to 1, but less than or equal to 300 sec. The default timeout is 10 sec.

Note: After you change VAP Minimal signal values, you must click **Update** to apply the changes and to save the settings.

5.10 «Fast Bss Transition» submenu

In order to ensure voice quality and network security, a portable station must be able to maintain a secure, low-latency voice call while roaming between APs that are handling other traffic.

The APs supports Fast BSS transition of the Station with WPA2 security.

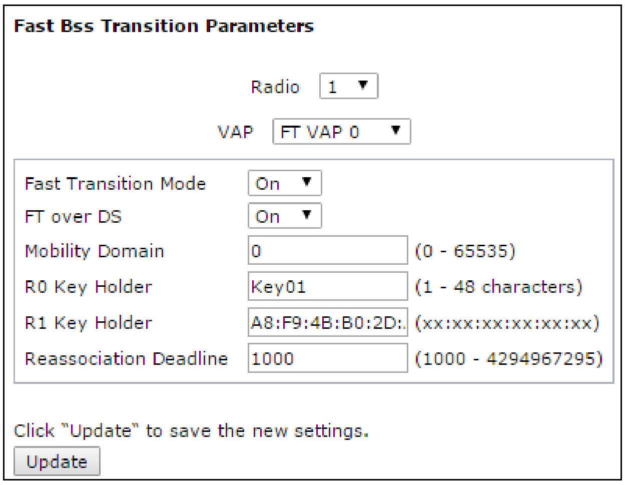
The AP supports Fast BSS Transition as defined in 802.11r for Fast handoff with WPA2 Enterprise security.

For Voice over Wi-Fi Enterprise only a subset of features defined in 802.11r is supported.

The need for Fast BSS transition is to decrease latency during roaming.

FBT is enabled per VAP per radio.

Note: Before you configure FBT on a VAP, be sure to verify that the VAP is configured with WPA2 security, pre-authentication disabled and MFP disabled.



Fast Bss Transition Parameters

Radio 1

VAP FT VAP 0

Fast Transition Mode	On	
FT over DS	On	
Mobility Domain	0	(0 - 65535)
R0 Key Holder	Key01	(1 - 48 characters)
R1 Key Holder	A8:F9:4B:B0:2D:	(xx:xx:xx:xx:xx:xx)
Reassociation Deadline	1000	(1000 - 4294967295)

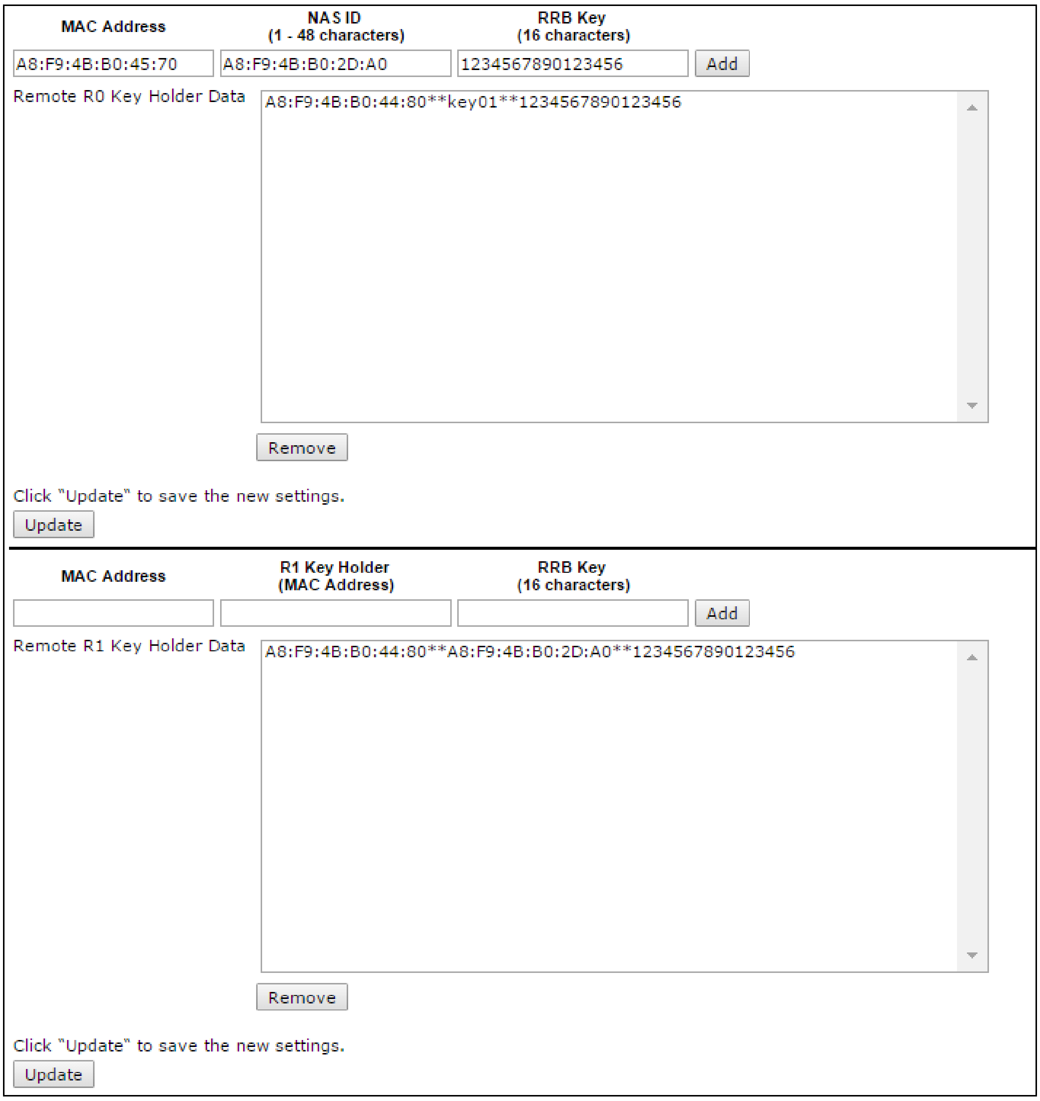
Click "Update" to save the new settings.

Field	Description
Radio	Select the radio on which FBT needs to be enabled.
VAP	Select the VAP on which FBT needs to be enabled.
Fast Transition Mode	Fast BSS Transition mode for the VAP. Flag to indicate whether FT authentication is permitted. The FT authentication is valid for WPA2 Personal or WPA2 Enterprise security. By default FBT mode is disabled.
FT over DS	You can enable or disable FT Over DS Mode. Enabling indicates support for FBT using Over-The-DS mechanism. By default FT over DS is disabled.
Mobility Domain	This defines the Mobility Domain identifier (MDID) of the FBT VAP. The MDID is used to indicate a group of APs within an ESS, between which a STA can use fast BSS transition services. Fast BSS transitions are allowed only between APs that have the same MDID and are within the same ESS. They are not allowed between APs with different MDIDs or in different ESSs. Default value is 0.
R0 Key Holder	The NAS identifier to be sent in radius Access Request Message. The NAS Identifier is used as R0 Key holder ID.
R1 Key Holder	The R1 key Holder ID that names the holder of PMK-R1 in the authenticator.

Reassociation Deadline	The time during which the target AP retains the PTKSA and any resources for a station while waiting for the Re-association request from the station. Default value is 1000 time units.

Note: After you configure the FBT settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

After specifying the basic settings you must configure the interaction between access points for rouming realizing by using MAC address and keys settings.



MAC Address	NAS ID (1 - 48 characters)	RRB Key (16 characters)	
A8:F9:4B:B0:45:70	A8:F9:4B:B0:2D:A0	1234567890123456	Add

Remote R0 Key Holder Data

A8:F9:4B:B0:44:80**key01**1234567890123456

Click "Update" to save the new settings.

MAC Address	R1 Key Holder (MAC Address)	RRB Key (16 characters)	
			Add

Remote R1 Key Holder Data

A8:F9:4B:B0:44:80**A8:F9:4B:B0:2D:A0**1234567890123456

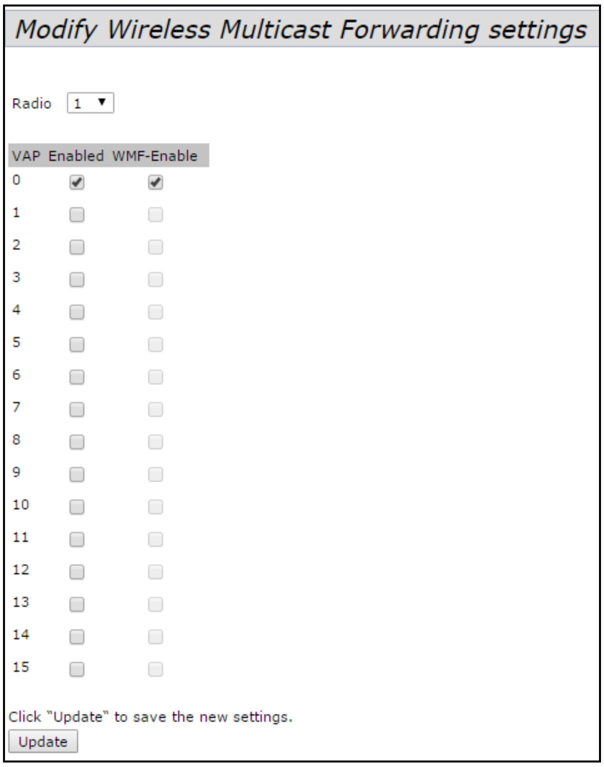
Click "Update" to save the new settings.

Field	*Description*
MAC Address	Destination's VAP MAC address which is the R1 Key holder. The PMKR1 is sent in RRB PUSH message to this AP MAC address. This MAC Address must be unique across all the VAPs.
R1 Key Holder	The R1 key Holder ID that names the holder of PMK-R1 in the authenticator.
RRB Key	Key used to encrypt RRM protocol messages.

Note: After you configure the FBT settings, you must click Update to apply the changes and to save the settings.

5.11 «Wireless Multicast Forwarding» submenu

The Wireless Multicast Forwarding provides an efficient way to forward the multicast traffic on the wireless medium and overcomes the multicast transmission issues on WLAN using the repeated unicast of multicast frames.



Modify Wireless Multicast Forwarding settings

Radio 1 ▼

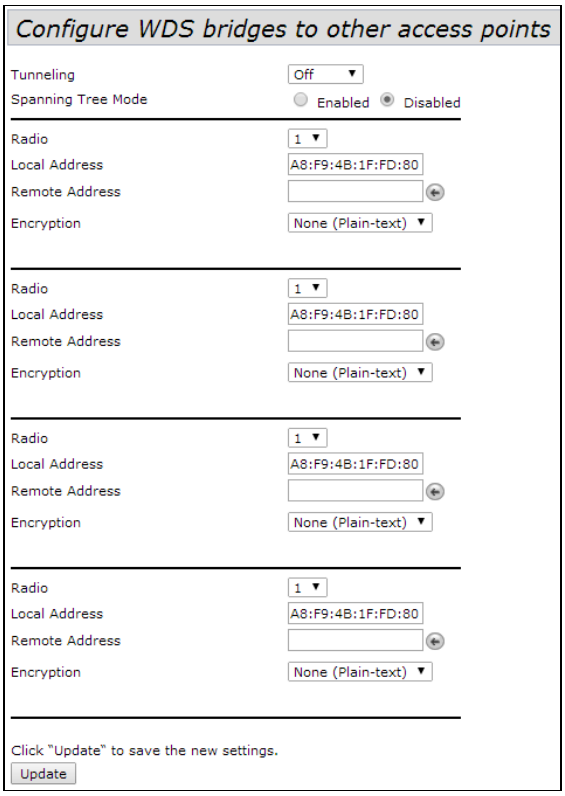
VAP	Enabled	WMF-Enable
0	☑	☑
1	□	□
2	□	□
3	□	□
4	□	□
5	□	□
6	□	□
7	□	□
8	□	□
9	□	□
10	□	□
11	□	□
12	□	□
13	□	□
14	□	□
15	□	□

Click "Update" to save the new settings.

Field	Description
VAP	You can configure up to 16 VAPs for each radio. You can configure up to 16 VAPs for each radio. VAP0 is the physical radio interface, so to disable VAP0, you must disable the radio.
Enabled	You can enable or disable a configured network. You can enable or disable a configured network. If you disable the specified network, you will lose the VLAN ID you enabled
WMF-Enable	Enable/Disable the WMF status in a VAP.

5.12 «WDS» submenu

To configure WDS on this AP, describe each AP intended to receive hand-offs and send information to this AP.



Configure WDS bridges to other access points

Tunneling: Off

Spanning Tree Mode: ○ Enabled ● Disabled

Radio: 1
Local Address: A8:F9:4B:1F:FD:80
Remote Address:
Encryption: None (Plain-text)

Radio: 1
Local Address: A8:F9:4B:1F:FD:80
Remote Address:
Encryption: None (Plain-text)

Radio: 1
Local Address: A8:F9:4B:1F:FD:80
Remote Address:
Encryption: None (Plain-text)

Radio: 1
Local Address: A8:F9:4B:1F:FD:80
Remote Address:
Encryption: None (Plain-text)

Click "Update" to save the new settings.

Tunneling – option is available only in case of GRE-using:

- *Off* – GRE is not used, Tunneling option is turned off;
- *Master* – point connects to the network via Ethernet-interface;
- *Slave* – point connects to the Master through radio interface;

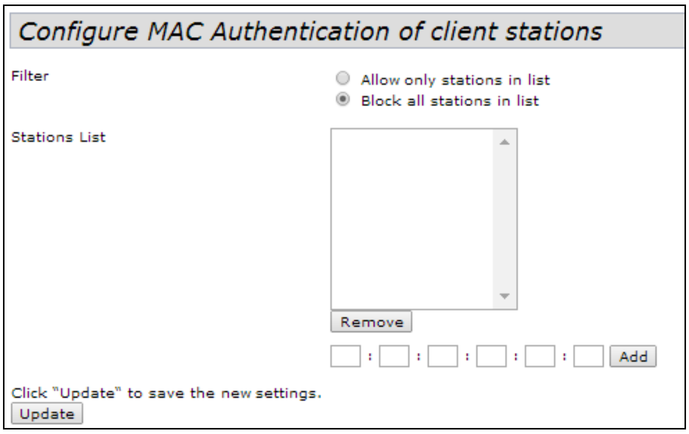
Field	*Description*
Spanning Tree Mode	Spanning Tree Protocol (STP) prevents switching loops. STP is recommended if youconfigure WDS links. Select **Enabled** to use STP Select **Disabled** to turn off STP links (not recommended)
Radio	For each WDS link on a two-radio AP, select Radio One or Radio Two. The rest of thesettings for the link apply to the radio selected in this *Field*. The read-only Local Address will change depending on which Radio you select in this *Field*.
Local Address	Indicates the MAC addresses for this AP. For each WDS link on a two-radio AP, the Local Address reflects the MAC address for theinternal interface on the selected radio (Radio One on wlan0 or Radio Two on wlan1).
Remote Address	Specify the MAC address of the destination AP; that is, the AP on the other end of the WDS link to which data will be sent or handed-off and from which data will be received. Click the drop-down arrow to the right of the **Remote Address** *Field* to see a list of all the available MAC Addresses and their associated SSIDs on the network. Select the appropriate MAC address from the list. **NOTE:** The SSID displayed in the drop-down list is simply to help you identify the

	correct MAC Address for the destination AP. This SSID is a separate SSID to that which you set for the WDS link. The two do not (and should not) be the same value or name.
Encryption	You can use no encryption or WPA (PSK) on the WDS link. If you are unconcerned about security issues on the WDS link you may decide not to set any type of encryption. Alternatively, if you have security concerns you can choose WPA (PSK). In WPA (PSK) mode, the AP uses WPA2-PSK with CCMP (AES) encryption over the WDS link. **NOTE:** In order to configure WPA-PSK on any WDS link, VAP0 of the selected radio must be configured for WPA-PSK or WPA-Enterprise.

Click **Update** to save the new settings.

5.13 «MAC Authentication» submenu

On the VAP page, the MAC Authentication Type setting controls whether the AP uses the station list configured locally on the MAC Authentication page or the external RADIUS server. The Allow/Block filter setting on the MAC Authentication page determines whether the clients in the station list (local or RADIUS) can access the network through the AP.



Configure MAC Authentication of client stations

Filter
○ Allow only stations in list
● Block all stations in list

Stations List

Click "Update" to save the new settings.

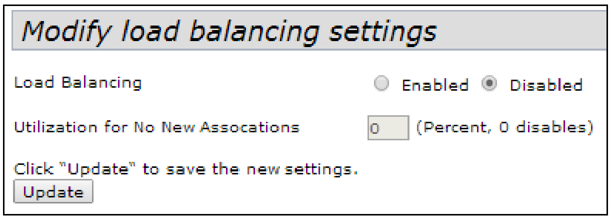
Field	***Description***
Filter	To set the MAC Address Filter, select one of the following options: • **Allow only stations in the list**. Any station that is not in the Stations List is denied access to the network through the AP. • **Block all stations in list**. Only the stations that appear in the list are denied access to the network through the AP. All other stations are permitted access. **Note:** The filter you select is applied to the clients in the station list, regardless of whether that station list is local or on the RADIUS server.
Stations List	This is the local list of clients that are either permitted or denied access to the network through the AP. To add a MAC Address to the local Stations List, enter its 48-bit MAC address into the lower text boxes, then click Add. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click Remove. The stations in the list will either be allowed or denied access based on how you set the filter in the previous *Field*. Please note that UAP allows upto 512 MAC addresses to be added to the station list. **Note:** If the MAC authentication type for the VAP is set to Local, the AP uses the Stations List to permit or deny the clients access to the network. If the MAC authentication type is set to RADIUS, the AP ignores the MAC addresses configured in this list and uses the list that is stored on the RADIUS server. The MAC authentication type is set on the VAP configuration page.

Note: After you configure local MAC Authentication settings, you must click **Update** to apply the changes and to save the settings. Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

Click **Update** to save the new settings.

5.14 «Load Balancing» submenu

You can set network utilization thresholds on the UAP 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.



Modify load balancing settings

Load Balancing ○ Enabled ● Disabled

Utilization for No New Assocations 0 (Percent, 0 disables)

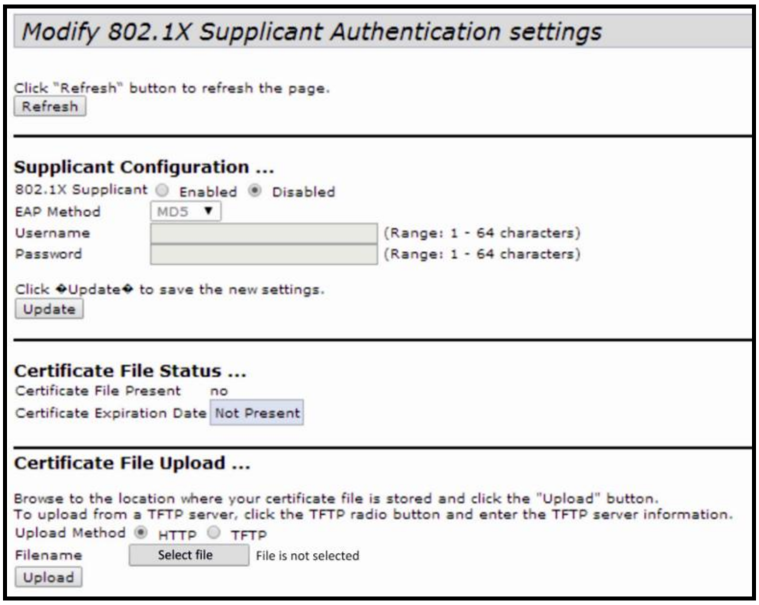
Click "Update" to save the new settings.

Field	Description
Load Balancing	Enable or disable load balancing: To enable load balancing on this AP, click **Enable**. To disable load balancing on this AP, click **Disable**.
Utilization for No NewAssociations	Provide 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 will be allowed regardless of the utilization rate.

Click **Update** to save the new settings.

5.15 «Authentication» submenu

Authentication settings allow the access point to gain access to a secured wired network. Use these settings to enable the access point as an 802.1X supplicant (client) on the wired network.



Modify 802.1X Supplicant Authentication settings

Click "Refresh" button to refresh the page.

Supplicant Configuration ...

802.1X Supplicant ○ Enabled ● Disabled

EAP Method MD5

Username (Range: 1 - 64 characters)

Password (Range: 1 - 64 characters)

Click ◆Update◆ to save the new settings.

Certificate File Status ...

Certificate File Present no

Certificate Expiration Date Not Present

Certificate File Upload ...

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method ● HTTP ○ TFTP

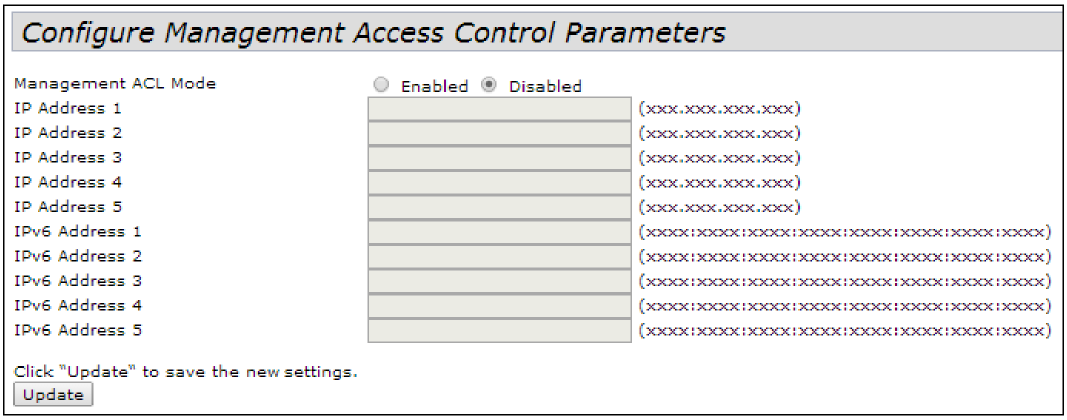
Filename File is not selected

Field	*Description*
Supplicant Configuration	
802.1X Supplicant	Click **Enabled** to enable the Administrative status of the 802.1X Supplicant. Click **Disabled** to disable the Administrative status of the 802.1X Supplicant.
EAP Method	Select the algorithm to be used for encrypting authentication user names and passwords. The options are as follows: • **MD5**—A hash function defined in RFC 3748 that provides basic security. • **PEAP**—Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel. • **TLS**—Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
Username	Enter the MD5 user name for the AP to use when responding to requests from an 802.1Xauthenticator. The user name can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Password	Enter the MD5 password for the AP to use when responding to requests from an 802.1Xauthenticator. The password can be 1 to 64 characters in length. ASCII printable characters are allowed, which includes upper and lower case letters, numbers, and special symbols such as @ and #.
Certificate File Status	
Certificate FilePresent	Indicates if the HTTP SSL Certificate file is present. Range is **Yes** or **No**. The default is **No.**
Certificate Expiration Date	Indicates when the HTTP SSL Certificate file will expire. The range is a valid date. If no certificate file exists on the AP, the *Field* displays *Not Present*.
Certificate File Upload	
Upload Method	Select the method to use for uploading a certificate file to the AP, which is either **HTTP**(upload by using a Web browser) or **TFTP** (upload by using a TFTP server).
Filename	Specify the path and filename of the certificate file: • For HTTP uploads, click **Browse** to browse to the location where the certificate file is stored, and then select the file to upload to the UAP. Click **Upload** to initiate the file transfer. • For TFTP uploads, enter the filename, including the path, of the certificate to upload to the UAP.
Server IP (TFTP Upload Only)	The IPv4 or IPv6 address of the TFTP server where the file is located. The default is 0.0.0.0. After you specify the filename and server IP, click **Upload** to initiate the file transfer.

Browse to the location where your certificate file is stored and click the «Upload» button.

5.16 «Management ACL» submenu

You can create an access control list (ACL) that lists up to five IPv4 hosts and five IPv6 hosts that are authorized to access the AP management interface. If this feature is disabled, anyone can access the management interface from any network client by supplying the correct AP username and password.



Configure Management Access Control Parameters

Management ACL Mode	○ Enabled ● Disabled	
IP Address 1		(xxx.xxx.xxx.xxx)
IP Address 2		(xxx.xxx.xxx.xxx)
IP Address 3		(xxx.xxx.xxx.xxx)
IP Address 4		(xxx.xxx.xxx.xxx)
IP Address 5		(xxx.xxx.xxx.xxx)
IPv6 Address 1		(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 2		(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 3		(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 4		(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 5		(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Click "Update" to save the new settings.

Field	*Description*
Management ACL Mode	Enable or disable the management ACL feature. At least one IPv4 or IPv6 address should be configured before enabling Management ACL Mode. If enabled, only the IP addresses you specify will have Web, Telnet, SSH, and SNMP access to the management interface.
IP Address (1-5)	Enter up to five IPv4 addresses that are allowed management access to the AP. Use dotted-decimal format (for example, 192.168.10.10).
IPv6 Address (1-5)	Enter up to five IPv6 addresses that are allowed management access to the AP. Use the standard IPv6 address format (for example 2001:0db8:1234::abcd).

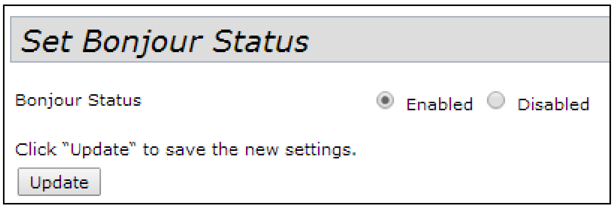
Note: After you configure the settings, click **Update** to apply the changes and to save the settings.

6 «SERVICES» MENU

Services menu provides settings of the integrated services for the access point.

6.1 «Bonjour» submenu

Bonjour is a software feature that allows the wireless access point and its services to be discovered on a local network using multicast Domain Name System (mDNS) service records. You can either enable or disable the Bonjour component system wide. The feature is not configurable on any specific network interface.



Set Bonjour Status

Bonjour Status ● Enabled ○ Disabled

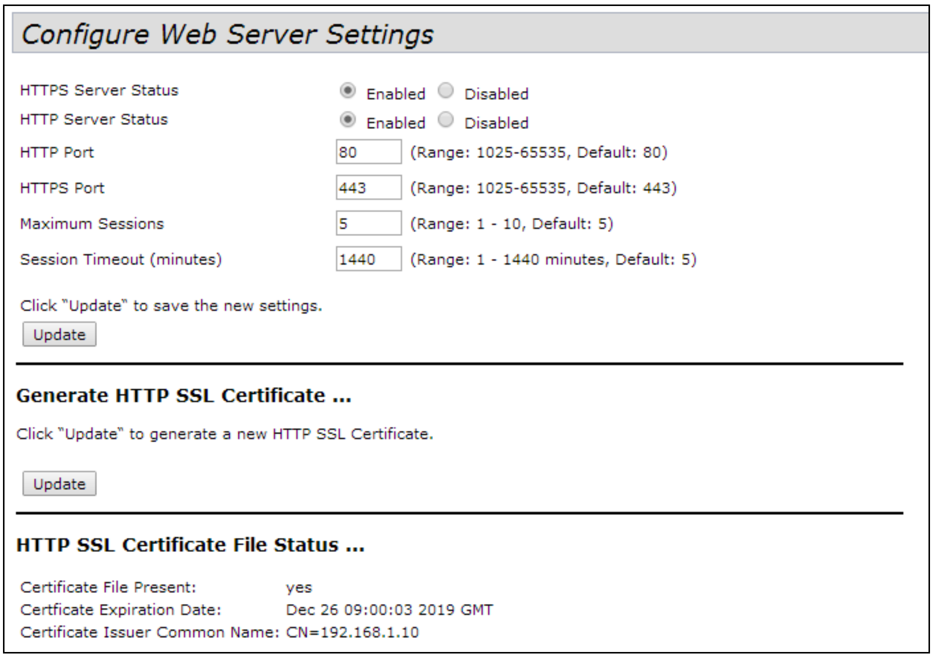
Click "Update" to save the new settings.

Field	Description
Bonjour Status	Enables or disables Bonjour. The default is **Enabled**.

Click **Update** to save the new settings.

6.2 «Web Server» submenu

Web Serves submenu provides access settings to the access point by Web-interface.



Configure Web Server Settings

HTTPS Server Status ● Enabled ○ Disabled

HTTP Server Status ● Enabled ○ Disabled

HTTP Port 80 (Range: 1025-65535, Default: 80)

HTTPS Port 443 (Range: 1025-65535, Default: 443)

Maximum Sessions 5 (Range: 1 - 10, Default: 5)

Session Timeout (minutes) 1440 (Range: 1 - 1440 minutes, Default: 5)

Click "Update" to save the new settings.

Generate HTTP SSL Certificate ...

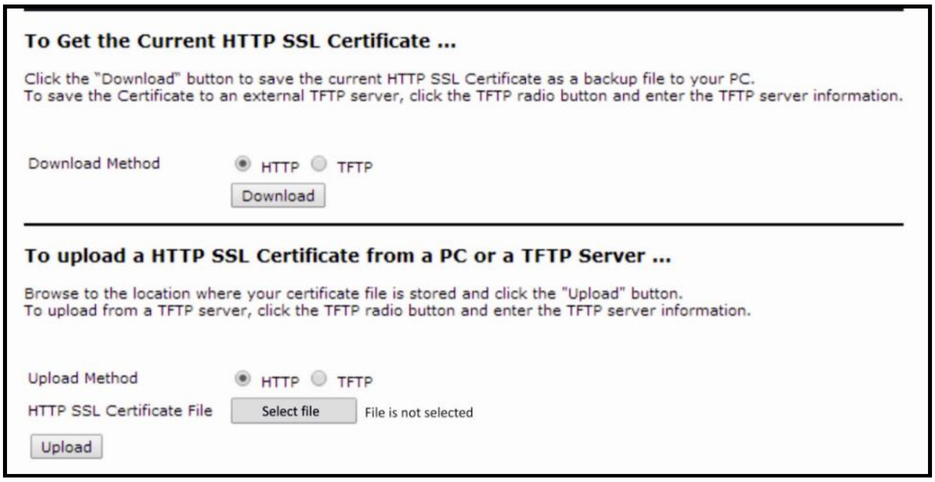
Click "Update" to generate a new HTTP SSL Certificate.

HTTP SSL Certificate File Status ...

Certificate File Present: yes

Certficate Expiration Date: Dec 26 09:00:03 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.10



To Get the Current HTTP SSL Certificate ...

Click the "Download" button to save the current HTTP SSL Certificate as a backup file to your PC.
To save the Certificate to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method ● HTTP ○ TFTP

To upload a HTTP SSL Certificate from a PC or a TFTP Server ...

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method ● HTTP ○ TFTP

HTTP SSL Certificate File: File is not selected

Field	*Description*
HTTPS Server Status	Enable or disable access through a Secure HTTP Server (HTTPS).
HTTP Server Status	Enable or disable access through HTTP. This setting is independent of the HTTPS serverstatus setting.
HTTP Port	Specify the port number for HTTP traffic (default is 80).
HTTPS Port	Specify the port number for HTTPS traffic (default is 443).
Maximum Sessions	When a user logs on to the AP web interface, a session is created. This session ismaintained until the user logs off or the session inactivity timer expires. Enter the number web sessions, including both HTTP and HTTPs, that can exist at the same time. The range is 1-10 sessions. The default is 5. If the maximum number of sessions is reached, the next user who attempts to log on to the AP web interface receives an error message about the session limit.
Session Timeout	Enter the maximum amount of time, in minutes, an inactive user remains logged on to the AP web interface. When the configured timeout is reached, the user is automatically logged off the AP. The range is 1-1440 minutes (1440 minutes = 1 day). The default is 60 minutes.

Click **Update** to save the new settings.

Generate HTTP SSL Certificate – click **Update** to generate a new HTTP SSL certificate for the secure Web server. This should be done once the access point has an IP address to ensure that the common name for the certificate matches the IP address of the UAP. Generating a new SSL certificate will restart the secure Web server. The secure connection will not work until the new certificate is accepted on the browser.

HTTP SSL Certificate File Status

Field	*Description*
Certificate FilePresent	Indicates if the HTTP SSL Certificate file is present. Range is either **Yes** or **No**. The default is**No**.
Certificate Expiration Date	Indicates when the HTTP SSL Certificate file will expire. The range is a valid date.
Certificate IssuerCommon Name	The Common name attribute of the server certificate. The range is a valid string.

To Get the Current HTTP SSL Certificate

Field	***Description***
Download Method	Select either **HTTP** or **TFTP** option. Click **Download** to save the current HTTP SSL Certificate as a backup file to your PC.
HTTP SSL CertificateFile	This *Field* is available when the selected download method is TFTP. Enter the filename of the certificate. The filename is a 255-byte alphanumeric string. The default is Mini_httpd.pem.
Server IP	The IPv4 or IPv6 address of the TFTP server where the file will be downloaded. The default is 0.0.0.0.

Click **Update** to generate a new HTTP SSL Certificate.

To Upload an HTTP SSL Certificate from a PC or a TFTP Server

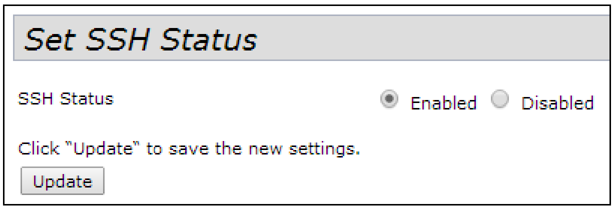
Field	***Description***
Upload Method	Select the upload method: • **HTTP**: Upload the file by using a Web browser • **TFTP**: Upload the file from a TFTP server
HTTP SSL CertificateFile	If the selected upload method is HTTP, the **Browse** button is available. Click the button to browse to the file to upload to the AP. If the selected upload method is TFTP, this *Field* displays a text box. Enter the filename of the certificate to upload to the AP.
Server IP	The IPv4 or IPv6 address of the TFTP server where the file is located. The default is 0.0.0.0.

Click the «Download» button to save the current HTTP SSL Certificate as a backup file to your PC. To save the Certificate to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

6.3 «SSH» submenu

Secure Shell (SSH) is a program that provides access to the FASTPATH UAP CLI from a remote host. SSH is more secure than Telnet for remote access because it provides strong authentication and secure communications over insecure channels. From the SSH page, you can enable or disable SSH access to the system.

SSH – secure protocl of the remote device management. SSH codifies all traffic including transmitted passwords in contrast with Telnet protocol.



Set SSH Status

SSH Status ● Enabled ○ Disabled

Click "Update" to save the new settings.

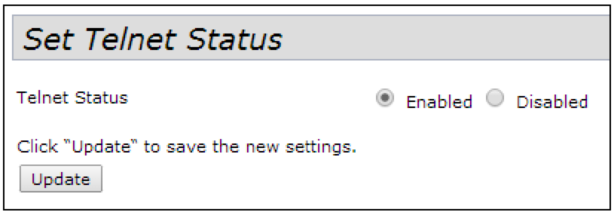
Field	***Description***
SSH Status	Choose to either enable or disable SSH access to the AP CLI: • To permit remote access to the AP by using SSH, click **Enabled**. • To prevent remote access to the AP by using SSH, click **Disabled**.

Click **Update** to save the new settings.

6.4 «Telnet» submenu

From the Telnet page, you can enable or disable Telnet access to the system.

Telnet – protocol for organizing of the control by a network. It allows you to connect from the computer to the gateway for settings and controlling.



Set Telnet Status

Telnet Status ● Enabled ○ Disabled

Click "Update" to save the new settings.

Field	***Description***
Telnet Status	Choose to either enable or disable Telnet access to the AP CLI: • To permit remote access to the AP by using Telnet, click **Enabled**. • To prevent remote access to the AP by using Telnet, click **Disabled**.

Click **Update** to save the new settings.

6.5 «QoS» submenu

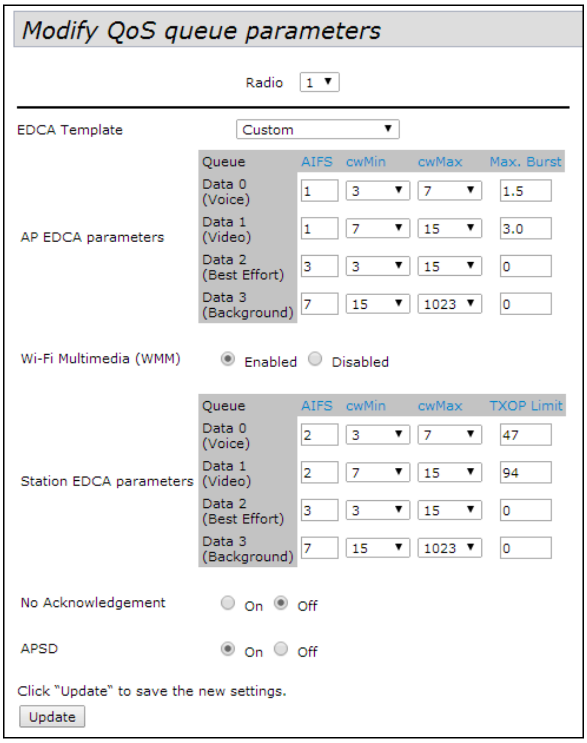
Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the UAP.

Configuring QoS on the UAP consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the AP only, not to that of the client stations.

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the AP to the client station.

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the AP.

Note: The QoS settings apply to both radios, but the traffic for each radio is queued independently.



Modify QoS queue parameters

Radio: 1

EDCA Template: Custom

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3.0
Data 2 (Best Effort)	3	3	15	0
Data 3 (Background)	7	15	1023	0

Wi-Fi Multimedia (WMM): ● Enabled ○ Disabled

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	3	15	0
Data 3 (Background)	7	15	1023	0

No Acknowledgement: ○ On ● Off

APSD: ● On ○ Off

Click "Update" to save the new settings.

Field	Description
Radio	Select the radio with the QoS settings to view or configure.
EDCA Template	The AP has multiple templates with predefined EDCA parameters. The menu includes the following templates: • Custom • Default • Optimized for Voice You can change the individual EDCA parameters only when the selected EDCAtemplate is Custom.
AP EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from AP-to-station: • **Data 0 (Voice)**-High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • **Data 1(Video)**-High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • **Data 2 (best effort)**-Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • **Data 3 (Background)**-Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 15.
cwMin (Minimum ContentionWindow)	This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified for Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the numberspecified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled.

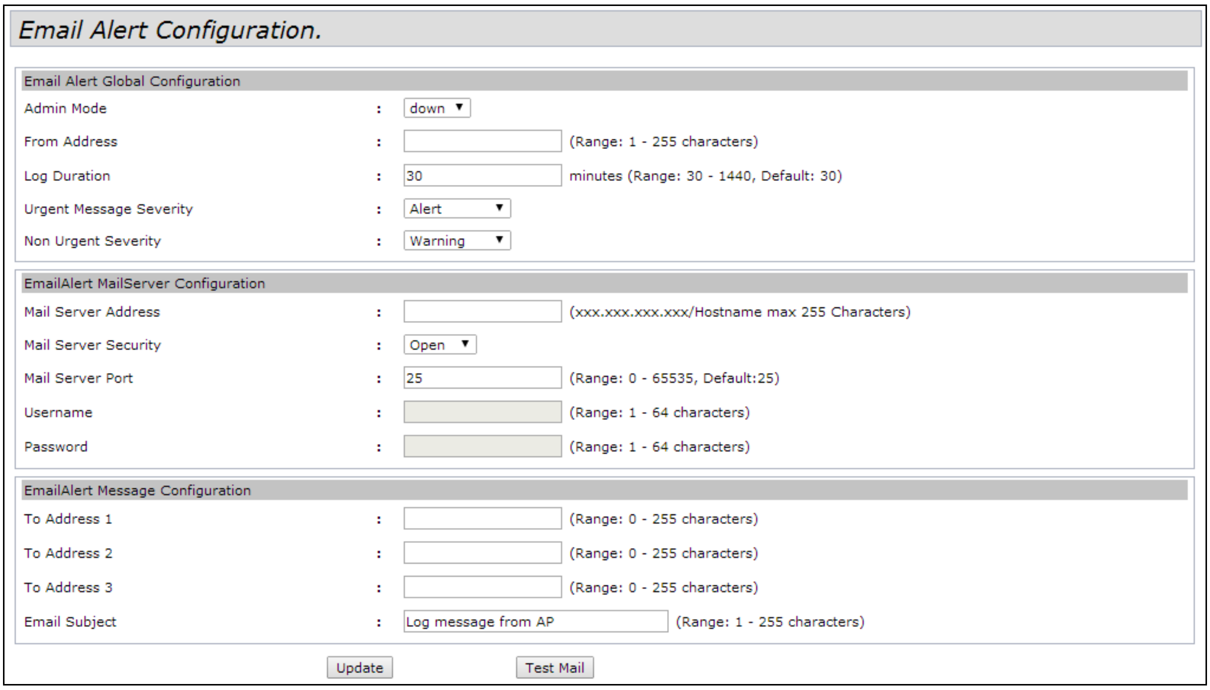
	Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for **cwMin** are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for cwMin must be lower than the value for cwMax.
cwMax (Maximum ContentionWindow)	The value specified for the Maximum Contention Window is the upper limit (inmilliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until amaximum number of retries allowed is reached. Valid values for **cwMax** are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. The value for cwMax must be higher than the value for cwMin.
Max. Burst Length	The **Max. Burst Length** is an AP EDCA parameter and only applies to traffic flowing from the AP to the client station. This value specifies (in milliseconds) the maximum burst length allowed for packetbursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999.
Wi-Fi Multimedia Settings	
Wi-Fi MultiMedia	Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the UAP control *downstream* traffic flowing from the AP to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the AP (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the AP. With WMM disabled, you can still set some parameters on the downstream trafficflowing from the AP to the client station (AP EDCA parameters). To disable WMM extensions, click **Disabled**. To enable WMM extensions, click **Enabled**.
Station EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from station-to-AP: • **Data 0 (Voice)**-Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • **Data 1(Video)**-Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • **Data 2 (best effort)**-Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • **Data 3 (Background)**-Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 15.
cwMin (Minimum ContentionWindow)	This parameter is used by the algorithm that determines the initial random backoff wait time (window) for retry of a data transmission during a period of contention for Unified Access Point resources. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time will be determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled.

	Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.
cwMax (Maximum ContentionWindow)	The value specified here in the Maximum Contention Window is the upper limit (inmilliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until amaximum number of retries allowed is reached.
TXOP Limit	The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the AP. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the Unified Access Point. The TXOP Limit maximum value is 65535.
Other QoS Settings	
No Acknowledgement	Select On to specify that the AP should not acknowledge frames with QosNoAck as the service class value.
APSD	Select On to enable Automatic Power Save Delivery (APSD), which is a powermanagement method. APSD is recommended if VoIP phones access the network through the AP.

Click **Update** to save the new settings.

6.6 «Email Alert» submenu

The Email Alert feature allows the AP to automatically send email messages when an event at or above theconfigured severity level occurs. Use the **Email Alert Configuration** page to configure mail server settings, to set the severity level that triggers alerts, and to add up to three email addresses where urgent and non-urgent email alerts are sent.



Email Alert Configuration.

Email Alert Global Configuration

Admin Mode : down

From Address : (Range: 1 - 255 characters)

Log Duration : 30 minutes (Range: 30 - 1440, Default: 30)

Urgent Message Severity : Alert

Non Urgent Severity : Warning

EmailAlert MailServer Configuration

Mail Server Address : (xxx.xxx.xxx.xxx/Hostname max 255 Characters)

Mail Server Security : Open

Mail Server Port : 25 (Range: 0 - 65535, Default:25)

Username : (Range: 1 - 64 characters)

Password : (Range: 1 - 64 characters)

EmailAlert Message Configuration

To Address 1 : (Range: 0 - 255 characters)

To Address 2 : (Range: 0 - 255 characters)

To Address 3 : (Range: 0 - 255 characters)

Email Subject : Log message from AP (Range: 1 - 255 characters)

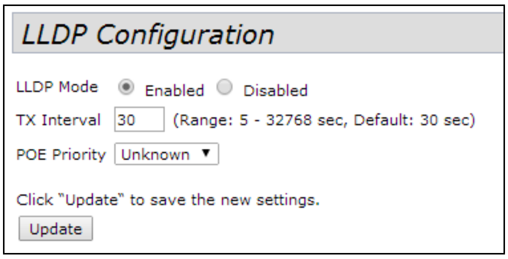
Field	*Description*
Email Alert Global Configuration	
Admin Mode	Globally enable or disable the Email Alert feature on the AP. By default, email alerts are disabled.
From Address	Specify the email address that appears in the *From Field* of alert messages sent from the AP, for example AP23@foo.com. The address can be a maximum of 255 characters and can contain only printable characters. By default, no address is configured.
Log Duration	This duration, in minutes, determines how frequently the non critical messages are sent to the SMTP Server. The range is 30-1440 minutes. The default is 30 minutes.
Urgent Message Severity	Configures the severity level for log messages that are considered to be urgent. Messages in this category are sent immediately. The security level you select and all higher levels are urgent:
Non Urgent Severity	Configures the severity level for log messages that are considered to be nonurgent. Messages in this category are collected and sent in a digest form at the time interval specified by the Log Duration *Field*. The security level you select and all levels up to, but not including the lowest Urgent level are considered nonurgent. Messages below the security level you specify are not sent via email. See the Urgent Message *Field Description* for information about the security levels.
Email Alert Mail Server Configuration	
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	Configures 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	Specify the username to use when authentication with the mail server is required. The username is a 64-byte character string with all printable characters. The default is**admin**.
Password	Specify the password associated with the username configured in the previous *Field*.
Email Alert Message Configuration	
To Address 1	Configure the first email address to which alert messages are sent.The address mustbe a valid email address. By default, no address is configured. The address can be a maximum of 255 characters and can contain only printable characters.
To Address 2	Optionally, configure the second email address to which alert messages are sent.Theaddress must be a valid email address. By default, no address is configured. The address can be a maximum of 255 characters and can contain only printable characters.
To Address 3	Optionally, configure the third email address to which alert messages are sent.Theaddress must be a valid email address. By default, no address is configured. The address can be a maximum of 255 characters and can contain only printable characters.
Email Subject	Specify the text to be displayed in the subject of the email alert message. The subjectcan contain up to 255 alphanumeric characters. The default is **Log message from AP.**

Note: After you configure the Email Alert settings, you must click **Update** to apply the changes and to save the settings.

To validate the configured email server credentials, click **Test Mail**. You can send a test email once the email server details are configured.

6.7 «LLDP» submenu

The Link Layer Discovery Protocol helps administrators track which devices are connected to each other. The Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) standardizes additional information elements that devices can pass to each other to improve network management. You can either Enable or Disable LLDP.



LLDP Configuration

LLDP Mode ● Enabled ○ Disabled

TX Interval 30 (Range: 5 - 32768 sec, Default: 30 sec)

POE Priority Unknown ▼

Click "Update" to save the new settings.

Field	***Description***
Lldp Mode	Enables or disables Lldp. The default is **Enabled**.
Transmit Interval	Specifies the number of seconds between LLDP message transmissions. Default value of Transmission interval is 30 seconds and configured from 5 to 32768
POE Priority	Indicates the priority level transmitted by the AP in the Extended Power information element. Priority can be configured as Low,High,Critical. Default value is Unknown

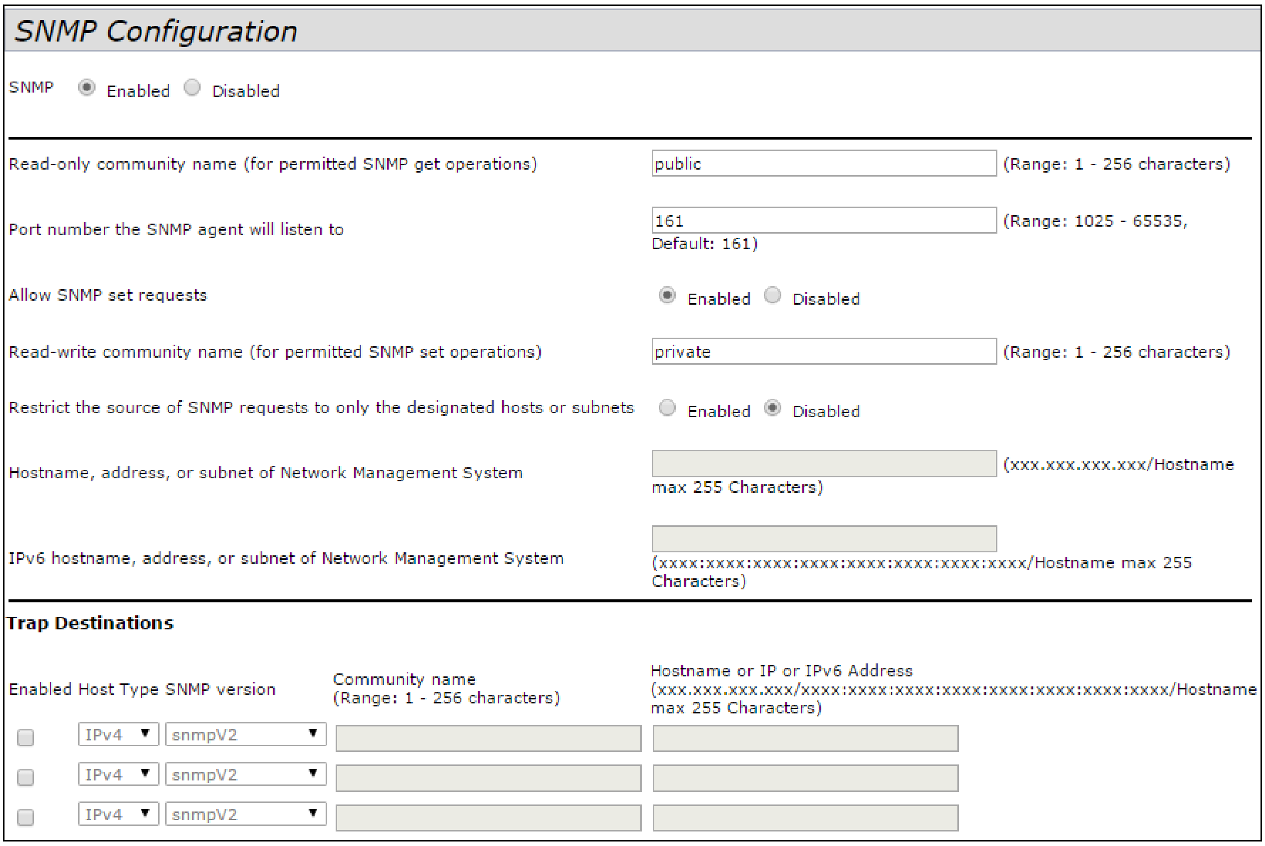
Click **Update** to save the new settings.

6.8 «SNMP» submenu

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The AP supports SNMP versions 1, 2, and 3. Unless specifically noted, all configuration parameters on this page apply to SNMPv1 and SNMPv2c only.

Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in Management Information Bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as APs, routers, switches, bridges, hubs, servers, or printers.

The UAP can function as an SNMP managed device for seamless integration into network management systems such as HP OpenView



SNMP Configuration

SNMP ● Enabled ○ Disabled

Read-only community name (for permitted SNMP get operations)	public (Range: 1 - 256 characters)
Port number the SNMP agent will listen to	161 (Range: 1025 - 65535, Default: 161)
Allow SNMP set requests	● Enabled ○ Disabled
Read-write community name (for permitted SNMP set operations)	private (Range: 1 - 256 characters)
Restrict the source of SNMP requests to only the designated hosts or subnets	○ Enabled ● Disabled
Hostname, address, or subnet of Network Management System	(xxx.xxx.xxx.xxx/Hostname max 255 Characters)
IPv6 hostname, address, or subnet of Network Management System	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters)

Trap Destinations

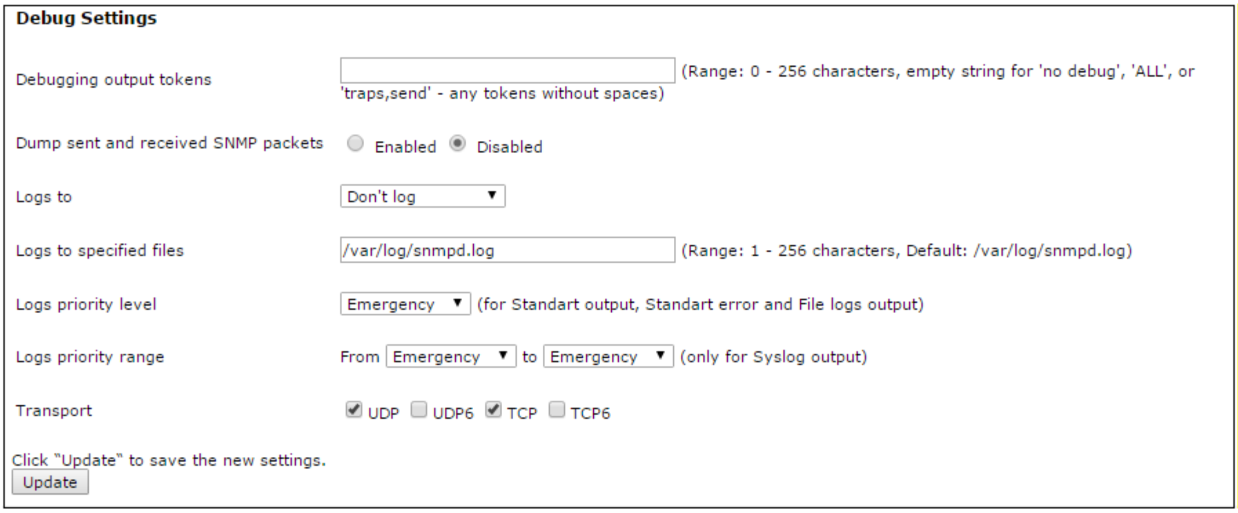
Enabled	Host Type	SNMP version	Community name (Range: 1 - 256 characters)	Hostname or IP or IPv6 Address (xxx.xxx.xxx.xxx/xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters)
□	IPv4 ▾	snmpV2 ▾		
□	IPv4 ▾	snmpV2 ▾		
□	IPv4 ▾	snmpV2 ▾		

Field	***Description***
SNMP Enabled/Disabled	You can specify the SNMP administrative mode on your network. By default SNMP is enabled. To enable SNMP, click **Enabled**.To disable SNMP, click **Disabled**. Afterchanging the mode, you must click **Update** to save your configuration changes. **Note**: If SNMP is disabled, all remaining *Field*s on the SNMP page are disabled. This is a global SNMP parameter which applies to SNMPv1, SNMPv2c, and SNMPv3.
Read-only community name (for permitted SNMP getoperations)	Enter a read-only community name. The valid range is 1-256 characters. The community name, as defined in SNMPv2c, acts as a simple authenticationmechanism to restrict the machines on the network that can request data to the SNMP agent. The name functions as a password, and the request is assumed to be authentic if the sender knows the password. The community name can be in any alphanumeric format.
Port number the SNMPagent will listen to	By default an SNMP agent only listens to requests from port 161. However, you canconfigure this so the agent listens to requests on another port. Enter the port number on which you want the SNMP agents to listen to requests. The valid range is 1-65535. **Note:** This is a global SNMP parameter that applies to SNMPv1, SNMPv2c, andSNMPv3.
Allow SNMP set requests	You can choose whether or not to allow SNMP set requests on the AP. Enabling SNMP set requests means that machines on the network can execute configuration changes via the SNMP agent on the AP to the Eltex System MIB. To enable SNMP set requests, click **Enabled**. To disable SNMP set requests, click **Disabled**.
Read-write communityname (for permitted SNMP set operations)	If you have enabled SNMP set requests you can set a read-write community name.The valid range is 1-256 characters. Setting a community name is similar to setting a password. Only requests from themachines that identify themselves with this community name will be accepted. The community name can be in any alphanumeric format.

Restrict the source ofSNMP requests to only the designated hosts orsubnets	You can restrict the source of permitted SNMP requests. To restrict the source of permitted SNMP requests, click **Enabled**. To permit any source submitting an SNMP request, click **Disabled**.
Hostname, address orsubnet of NetworkManagement System	Specify the IPv4 DNS hostname or subnet of the machines that can execute get and set requests to the managed devices. The valid range is 1-256 characters. As with community names, this provides a level of security on SNMP settings. TheSNMP agent will only accept requests from the hostname or subnet specified here. To specify a subnet, enter one or more subnetwork address ranges in the formaddress/mask_length where *address* is an IP address and *mask_length* is the number of mask bits. Both formats address/mask and address/mask_length are supported. Individual hosts can be provided for this, i.e. I.P Address or Hostname. For example, if you enter a range of 192.168.1.0/24 this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0. The address range is used to specify the subnet of the designated NMS. Onlymachines with IP addresses in this range are permitted to execute get and set requests on the managed device. Given the example above, the machines with addresses from 192.168.1.1 through 192.168.1.254 can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by .255 in the range is always reserved for the broadcast address). As another example, if you enter a range of 10.10.1.128/25 machines with IPaddresses from 10.10.1.129 through 10.10.1.254 can execute SNMP requests on managed devices. In this example, 10.10.1.128 is the network address and 10.10.1.255 is the broadcast address. 126 addresses would be designated.
IPv6 Hostname or IPv6subnet of Network Management System	Specify the IPv6 DNS hostname or subnet of the machines that can execute get andset requests to the managed devices.
Community name for traps	Enter the global community string associated with SNMP traps. The valid range is 1-256 characters. Traps sent from the device will provide this string as a community name. The community name can be in any alphanumeric format. Special characters are not permitted.
Host Type	Specify whether the enabled host is an IPv4 host or an IPv6 host.
Hostname or IP address	Enter the DNS hostname of the computer to which you want to send SNMP traps. The valid range is 1-256 characters. An example of a DNS hostname is: snmptraps.foo.com. Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can add up to a maximum of three DNS hostnames. Ensure you select the **Enabled** check box beside the appropriate hostname.

Click **Update** to save the new settings.

«**Debug Settings**» subchapter provides settings of the debugging message sending



Debug Settings

Debugging output tokens [ ] (Range: 0 - 256 characters, empty string for 'no debug', 'ALL', or 'traps,send' - any tokens without spaces)

Dump sent and received SNMP packets ○ Enabled ● Disabled

Logs to: Don't log

Logs to specified files: /var/log/snmpd.log (Range: 1 - 256 characters, Default: /var/log/snmpd.log)

Logs priority level: Emergency (for Standart output, Standart error and File logs output)

Logs priority range: From Emergency to Emergency (only for Syslog output)

Transport: ☑ UDP ☐ UDP6 ☑ TCP ☐ TCP6

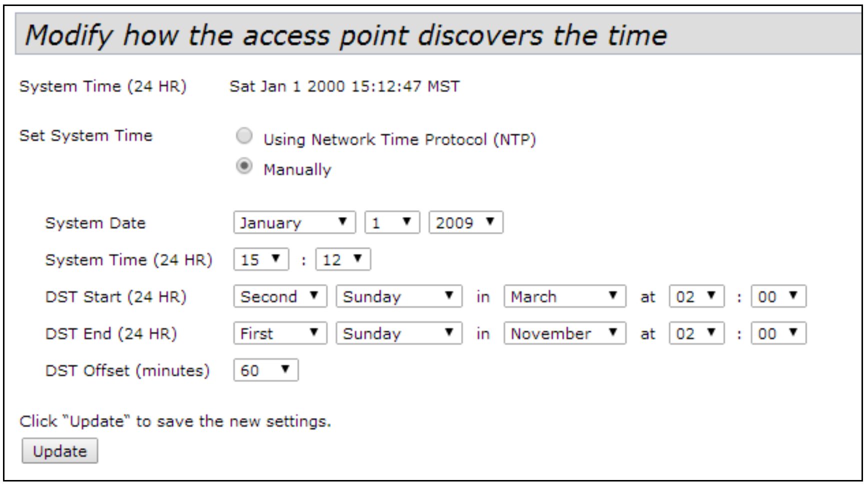
Click "Update" to save the new settings.

Field	Description
Debugging output tokens	Identificator of the debagging message group.
Dump sent and received SNMP packets	Sent and received SNMP packets that are dumped into log.
Logs to	Entering of the log place for dumping: ▪ *Don't log* – not show log; ▪ Standart error, standart output – output in the console; ▪ File – output in the file; ▪ Syslog – Syslog-output;
Logs to specified files	Specify file for log output.
Logs priority level	Specify level for output logs (it is assigned if log is output in the console or file).
Logs priority range	Entering of the log range levels for Syslog-output.
Transport	Transport protocol for SNMP-message transmission.

Click **Update** button to save introduction of modifications.

6.9 «Time Settings (NTP)» submenu

The Network Time Protocol (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. 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. The timestamp is used to indicate the date and time of each event in log messages.



Modify how the access point discovers the time

System Time (24 HR) Sat Jan 1 2000 15:12:47 MST

Set System Time ○ Using Network Time Protocol (NTP)
● Manually

System Date January 1 2009

System Time (24 HR) 15 : 12

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

Click "Update" to save the new settings.

Update

Field	*Description*
Set System Time	Specify how to set the system time.
NTP Server	If NTP is enabled, specify the NTP server to use. You can specify the NTP server by hostname, IPv4 address, or IPv6 address, although using the IPv4/IPv6 address is not recommended as these can change more readily. If you specify a hostname, note the following requirements: A hostname can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a hostname includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.
Time Zone	Select your local time zone from the menu. The default is **USA (Pacific)**.
Adjust Time for DaylightSavings	Select this option to have the system adjust the reported time for Daylight Savings Time (DST), which is also known as Summer Time. When this *Field* is selected, *Fields* to configure Daylight Savings Time settings appear.
DST Start (24 HR)	Configure the date and time to begin Daylight Savings Time for the System Time.
DST End (24 HR)	Configure the date and time to end Daylight Savings Time for the System Time.
DST Offset (minutes)	Select the number of minutes to offset DST. The default is **60** minutes.

Click **Update** to save the new settings.

7 «SNMPV3» MENU

«SNMPv3» menu is destined for configuring of the license interaction with device hardware and software via SNMPv3 protocol.

7.1 Подменю «SNMPv3 Views»

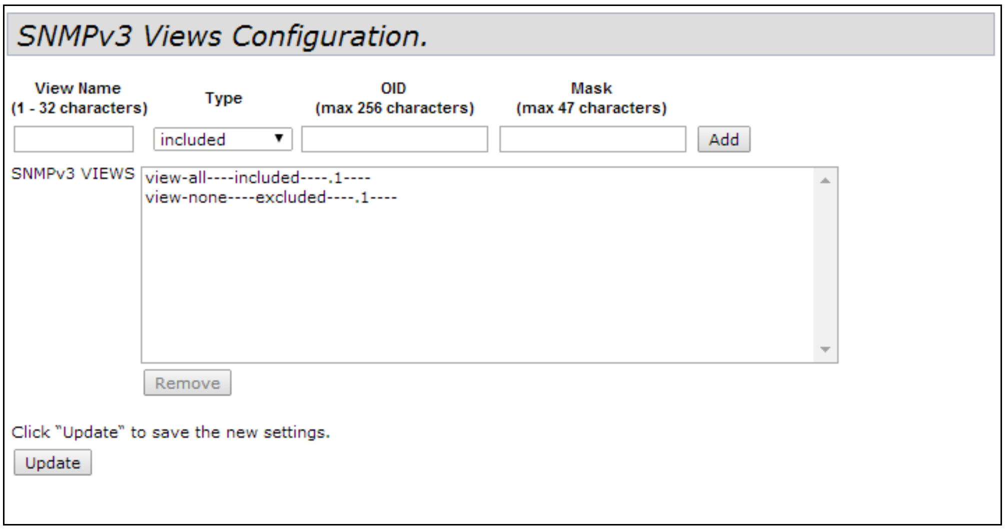
A MIB view is a family of view subtrees, which is a pairing of an OID subtree value together with a bit string mask value. Each MIB view is defined by two sets of view subtrees, included in or excluded from the MIB view. You can create MIB views to control the OID range that SNMPv3 users can access.

Note that the UAP supports a maximum of 16 views.

The following notes summarize some critical guidelines regarding SNMPv3 View configuration. Please read all the notes before proceeding with SNMPv3 View configuration.

Note: A MIB view called all is created by default in the system. This view contains all management objects supported by the system.

Note: By default, view-all and view-none SNMPv3 views are created on the AP. These views cannot be deleted but OID, Masks and Type *Field*s can be modified.



SNMPv3 Views Configuration.

View Name (1 - 32 characters)	Type	OID (max 256 characters)	Mask (max 47 characters)	
	included ▼			Add

SNMPv3 VIEWS
view-all----included----.1----
view-none----excluded----.1----

Click "Update" to save the new settings.

Field	*Description*
View Name	Enter a name to identify the MIB view. View names can contain up to 32 alphanumeric characters and can include hyphens.
Type	Specifies whether to include or exclude the view subtree or family of subtrees from the MIB view.
OID	Enter an OID string for the subtree to include or exclude from the view. For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.
Mask	The OID mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... orxx:xx:xx.... (:) and is 16 octets in length. Each octet is 2 hexadecimal characters separated by either . (period) or : (colon). Only hex characters are accepted in this *Field*. For example, OID mask FA.80 is 11111010.10000000. A family mask is used to define a family of view subtrees. The family mask indicates whichsub-identifiers of the associated family OID string are significant to the family's definition.

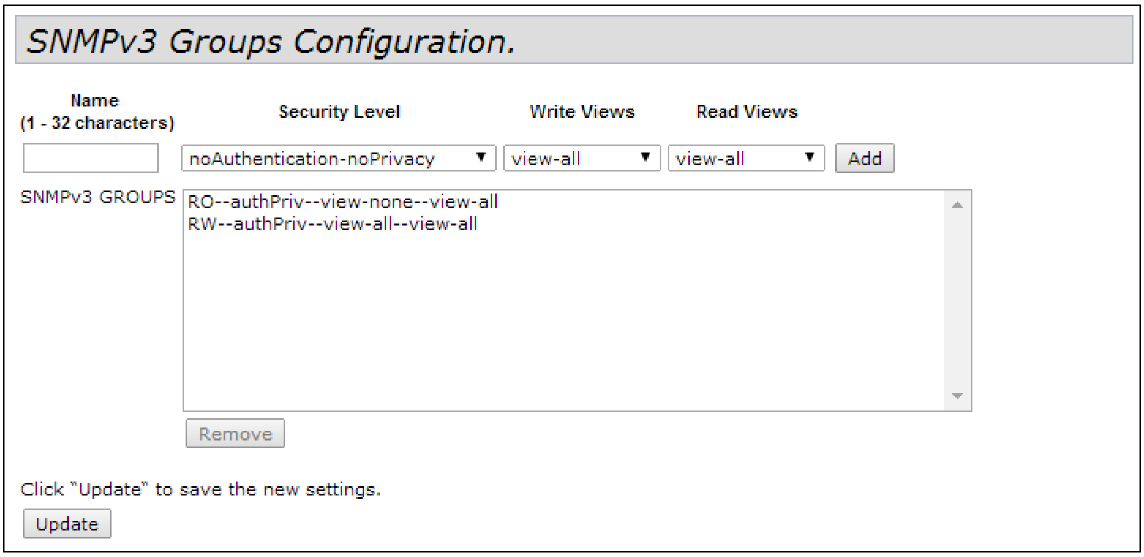
	A family of view subtrees allows control access to one row in a table, in a more efficientmanner.
SNMPv3 Views	This *Field* shows the MIB views on the UAP.

Use the buttons on the page to perform the following tasks:

- **Add**: Add the new view to the SNMPv3 Views table.
- **Remove**: Remove the selected view from the SNMPv3 Views table.
- **Update**: Apply and save the changed SNMPv3 view settings.

7.2 «SNMPv3 Groups» submenu

SNMPv3 groups allow you to combine users into groups of different authorization and access privileges.



SNMPv3 Groups Configuration.

Name (1 - 32 characters):

Security Level: noAuthentication-noPrivacy

Write Views: view-all

Read Views: view-all

SNMPv3 GROUPS:
RO--authPriv--view-none--view-all
RW--authPriv--view-all--view-all

Click "Update" to save the new settings.

Field	***Description***
Name	Specify a name to use to identify the group. The default group names are RW and RO. Group names can contain up to 32 alphanumeric characters and can include hyphens.
Security Level	Select one of the following security levels for the group: • **noAuthentication-noPrivacy**-No authentication and no data encryption (no security). • **Authentication-noPrivacy**-Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption. • **Authentication-Privacy**-Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption. For groups that require authentication, encryption, or both, you must define the MD5 and DES key/passwords on the **SNMPv3 Users** page.
Write Views	Select the write access to management objects (MIBs) for the group: • **write-all**-The group can create, alter, and delete MIBs. • **write-none**-The group is not allowed to create, alter, or delete MIBS.
Read Views	Select the read access to management objects (MIBs) for the group: • **view-all**-The group is allowed to view and read all MIBs. • **view-none**-The group cannot view or read MIBs.

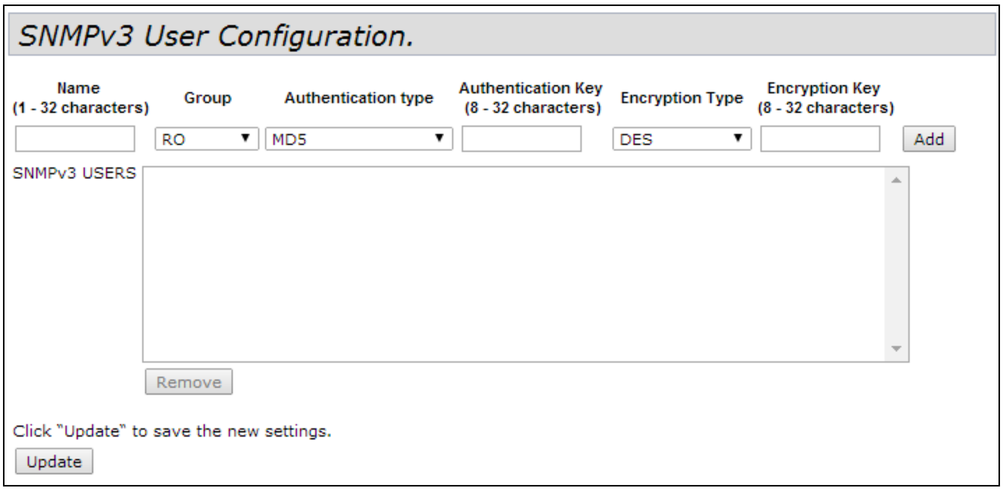
SNMPv3 Groups	This *Field* shows the default groups and the groups that have been defined on the AP.

Use the buttons on the page to perform the following tasks:

- **Add**: Add the new group to the SNMPv3 Groups table.
- **Remove**: Remove the selected group from the SNMPv3 Group table.
- **Update**: Apply and save the changed SNMPv3 group settings.

7.3 «SNMPv3 Users» submenu

From the **SNMPv3 Users** page, you can define multiple users, associate the desired security level to each user, and configure per user security keys.



SNMPv3 User Configuration.

Name (1 - 32 characters)	Group	Authentication type	Authentication Key (8 - 32 characters)	Encryption Type	Encryption Key (8 - 32 characters)	
	RO	MD5		DES		Add

Click "Update" to save the new settings.

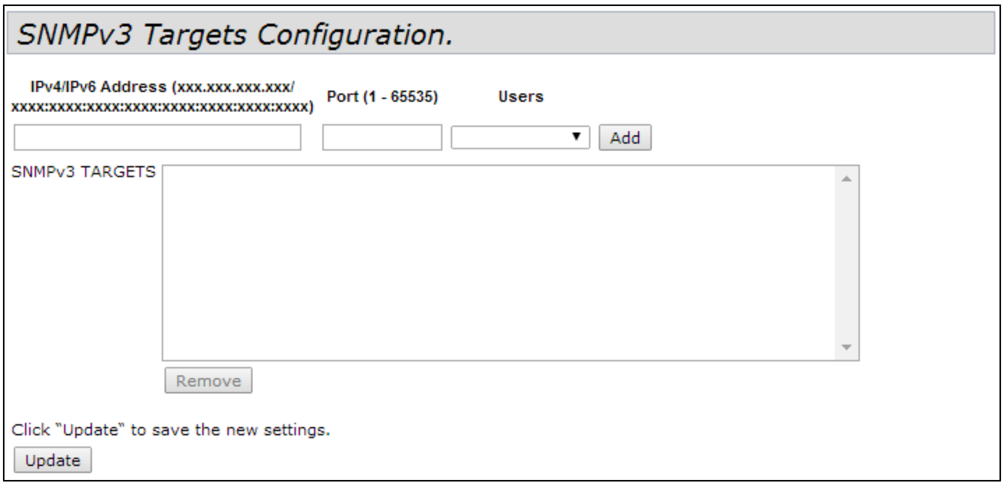
Field	*Description*
Name	Enter the user name to identify the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
Group	Map the user to a group. The default groups are RW and RO. You can define additionalgroups on the **SNMPv3 Groups** page.
Authentication Type	Select the type of authentication to use on SNMP requests from the user: • **MD5**-Require MD5 authentication on SNMPv3 requests from the user. • **None**-SNMPv3 requests from this user require no authentication.
Authentication Key	If you specify **MD5** as the authentication type, enter a password to enable the SNMP agent to authenticate requests sent by the user. The passphrase must be between 8 and 32 characters in length.
Encryption Type	Select the type of privacy to use on SNMP requests from the user: • **DES**-Use DES encryption on SNMPv3 requests from the user. • **None**-SNMPv3 requests from this user require no privacy.
Encryption Key	If you specify **DES** as the privacy type, enter a key to use to encrypt the SNMP requests. The passphrase must be between 8 and 32 characters in length.
SNMPv3 Users	This *Field* shows the users that have been defined on the AP.

Use the buttons on the page to perform the following tasks:

- **Add**: Add the new user to the SNMPv3 Users table.
- **Remove**: Remove the selected user from the SNMPv3 Users table.
- **Update**: Apply and save the changed SNMPv3 user settings.

7.4 «SNMPv3 Targets» submenu

An SNMPv3 targets receives trap messages and forwards them to the SNMP manager. Inform messages are not supported. Each target is associated with target IP address, UDP port, and SNMPv3 user name.



SNMPv3 Targets Configuration.

IPv4/IPv6 Address (xxx.xxx.xxx.xxx/ xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
Port (1 - 65535)
Users
Add
SNMPv3 TARGETS
Remove

Click "Update" to save the new settings.

Field	*Description*
IPv4/IPv6 Address	Enter the IP address of the remote SNMP target (receiver).
Port	Enter the UDP port to use for sending SNMP targets.
Users	Enter the name of the SNMP user to associate with the target.
SNMPv3 Targets	This *Field* shows the SNMPv3 targets configured on the UAP.

Use the buttons on the page to perform the following tasks:

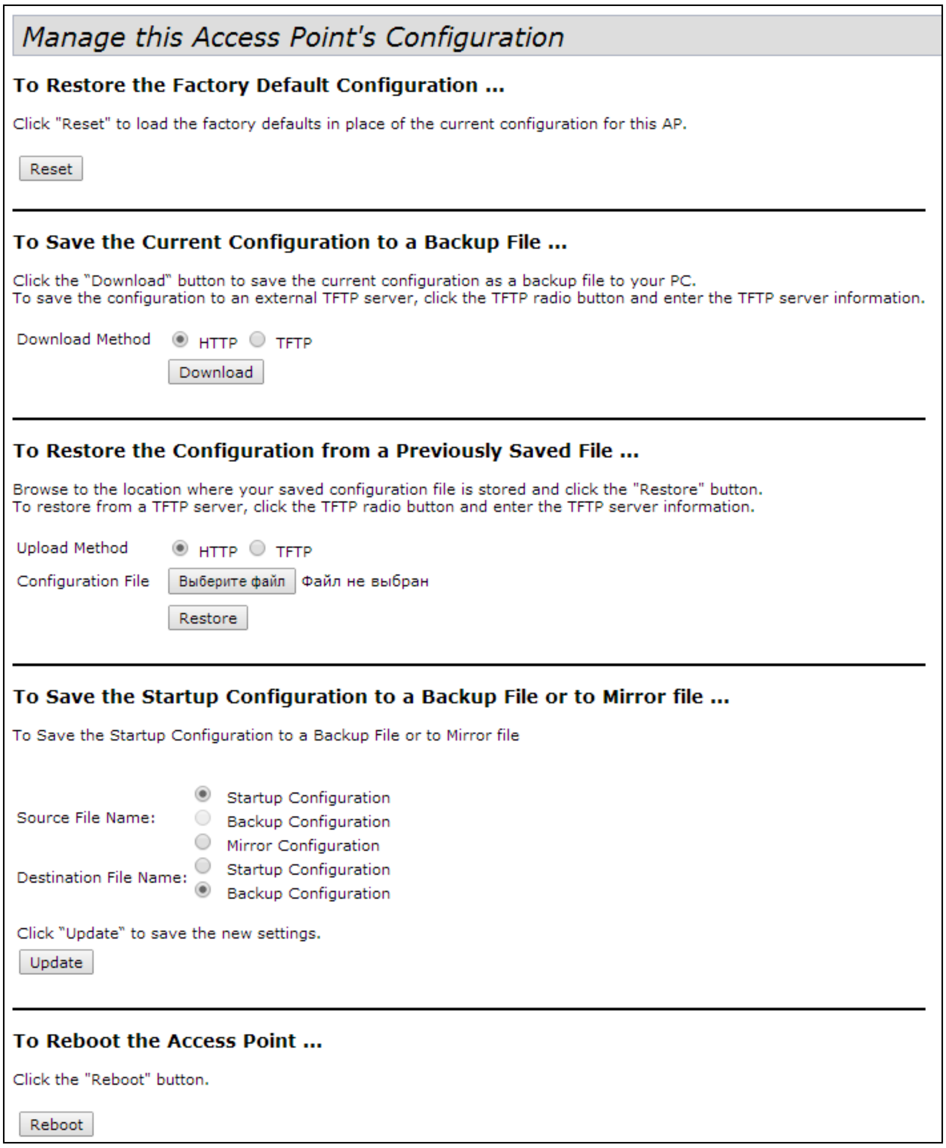
- **Add**: Add the new target to the SNMPv3 Targets table.
- **Remove**: Remove the selected target from the SNMPv3 Targets table.
- **Update**: Apply and save the changed SNMPv3 target settings.

8 «MAINTENANCE» MENU

The WEB-interface section is destined for device common control: unloading, loading, configuration settings as a default, software updating, device reboot; and for debugging operations: traffic sniffing propagated through the access point and unloading of the diagnostic information via the device.

8.1 «Configuration» submenu

The UAP configuration file is in XML format and contains all of the information about the AP settings. You can download the configuration file to a management station to manually edit the content or to save as a back-up copy. When you upload a configuration file to the AP, the configuration information in the XML file is applied to the AP.



Manage this Access Point's Configuration

To Restore the Factory Default Configuration ...

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

Reset

To Save the Current Configuration to a Backup File ...

Click the "Download" button to save the current configuration as a backup file to your PC.
To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method ● HTTP ○ TFTP

Download

To Restore the Configuration from a Previously Saved File ...

Browse to the location where your saved configuration file is stored and click the "Restore" button.
To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method ● HTTP ○ TFTP

Configuration File Выберите файл Файл не выбран

Restore

To Save the Startup Configuration to a Backup File or to Mirror file ...

To Save the Startup Configuration to a Backup File or to Mirror file

Source File Name: ● Startup Configuration
○ Backup Configuration
○ Mirror Configuration

Destination File Name: ○ Startup Configuration
● Backup Configuration

Click "Update" to save the new settings.

Update

To Reboot the Access Point ...

Click the "Reboot" button.

Reboot

If you are experiencing problems with the UAP and have tried all other troubleshooting measures, click **Reset**. This restores factory defaults and clears all settings, including settings such as a new password or wireless settings. You can also use the reset button on the back panel to reset the system to the default configuration.

Restore the Factory Default Configuration

If you are experiencing problems with the UAP and have tried all other troubleshooting measures, click **Reset**. This restores factory defaults and clears all settings, including settings such as a new password or wireless settings. You can also use the reset button on the back panel to reset the system to the default configuration.

Saving the Current Configuration to a Backup File

You can use HTTP or TFTP to transfer files to and from the UAP. After you download a configuration file to the management station, you can manually edit the file, which is in XML format. Then, you can upload the edited configuration file to apply those configuration settings to the AP.

Use the following steps to save a copy of the current settings on an AP to a backup configuration file by using TFTP:

1. Select **TFTP** for **Download Method**
2. Enter a name (1 to 255 characters) for the backup file in the **Filename** *Field*, including the .xml file name extension and the path to the directory where you want to save the file. File name should not contain spaces, <, >, |, \, : , (,), &, ; , #, ? , * and successive '.' .
3. Enter the IP address of the TFTP server.
4. Click **Download** to save the file.

Use the following steps to save a copy of the current settings on an AP to a backup configuration file by using HTTP:

1. Select **HTTP** for **Download Method**.
2. Click the **Download** button. A dialog box displays verifying the download.
3. To proceed with the download, select **OK**. A dialog box opens allowing you to view or save the file.
4. Select the **Save File** option and select **OK**.
5. Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

You can keep the default file name (config.xml) or rename the backup file, but be sure to save the file with an .xmlextension.

Restoring the Configuration from a Previously Saved File

You can use HTTP or TFTP to transfer files to and from the UAP. After you download a configuration file to the management station, you can manually edit the file, which is in XML format. Then, you can upload the edited configuration file to apply those configuration settings to the AP.

Configuration cannot be uploaded to an AP unless the model, number of radios and their configurable modes match.

Use the following procedures to restore the configuration on an AP to previously saved settings by using TFTP:

1. Select **TFTP** for **Upload Method**.
2. Enter a name (1 to 255 characters) for the backup file in the **Filename** *Field*, including the .xml file name extension and the path to the directory that contains the configuration file to upload. File name should not contain spaces, <, >, |, \, : , (,), &, ; , #, ? , * and successive '.'
3. Enter the IP address of the TFTP server in the **Server IP** *Field*.

4. Click the **Restore** button.

The AP reboots. A reboot confirmation dialog and follow-on rebooting status message displays. Please wait for the reboot process to complete, which might take several minutes.

The Administration Web UI is not accessible until the AP has rebooted.

Use the following steps to save a copy of the current settings on an AP to a backup configuration file by using HTTP:

1. Select **HTTP** for **Upload Method**.
2. User the **Browse** button to select the file to restore.
3. Click the **Restore** button. A File Upload or Choose File dialog box displays.
4. Navigate to the directory that contains the file, then select the file to upload and click **Open** (Only those files created with the Backup function and saved as .xml backup configuration files are valid to use with Restore; for example, ap_config.xml.)
5. Click the **Restore** button. A dialog box opens verifying the restore.
6. Click **OK** to proceed.

The AP reboots. A reboot confirmation dialog and follow-on rebooting status message displays. Please wait for the reboot process to complete, which might take several minutes.

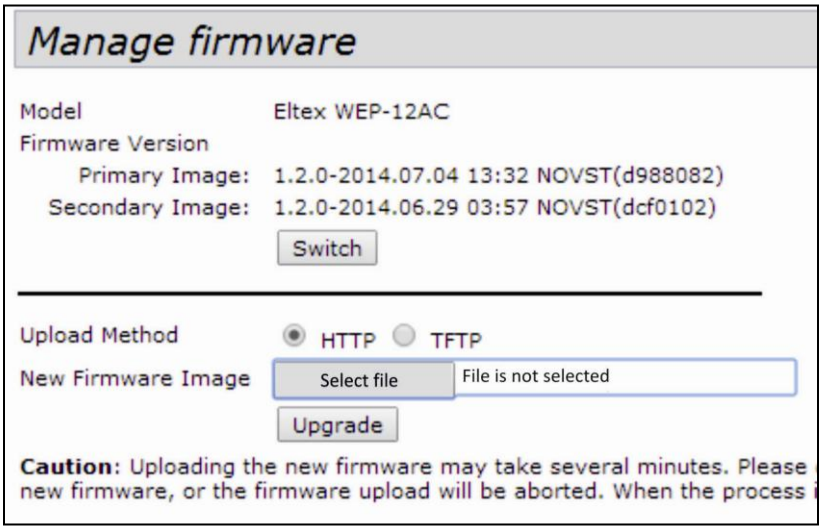
The Administration Web UI is not accessible until the AP has rebooted.

Rebooting the Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the UAP. To reboot the access point, click the **Reboot** button on the **Configuration** page.

8.2 «Upgrade» submenu

Use this page to select the firmware image that the AP loads when it boots and to upload a new firmware image to the device. The AP always tries to boot with the primary image. If the primary image fails to load, then the secondary image is used to load the AP. Whenever such a failover occurs, the system creates a log message to help you troubleshoot the firmware failure.



Manage firmware

Model Eltex WEP-12AC

Firmware Version

Primary Image: 1.2.0-2014.07.04 13:32 NOVST(d988082)

Secondary Image: 1.2.0-2014.06.29 03:57 NOVST(dcf0102)

Switch

Upload Method ● HTTP ○ TFTP

New Firmware Image Select file File is not selected

Upgrade

Caution: Uploading the new firmware may take several minutes. Please
new firmware, or the firmware upload will be aborted. When the process

Field	Description
Model	The product identifier.
Firmware Version	Identifies the firmware images on the system: - **Primary Image**—The version number of the image that is loaded during system boot. - **Secondary Image—**The version number of the secondary (backup) image on the system.
Upload Method	The method to use to upload a new firmware image to the AP: - **HTTP—**Use a Web browser. - **TFTP—**Use a TFTP server.
New Firmware Image(HTTP Upload)	Click **Browse** to browse to and select the new firmware image located on an administrative system.
Image Filename (TFTPUpload)	The path and filename of the firmware image to upload to the AP. Only filenames with extension .tar will be uploaded to ap.
Server IP (TFTP Upload)	The IP address of the TFTP server where the new firmware image is located.

Use the buttons to perform the following tasks:

- **Switch:** Use the secondary image as the primary image. The change takes effect the next time the AP boots. For more information, see Switch Firmware Image.
- **Upgrade:** Upload the specified firmware image to the AP. For more information about the firmware upgrade procedures, see Upgrade Firmware.

The process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the image switch is in process. When the image switch is complete, the access point restarts. The AP resumes normal operation with the same configuration settings it had before the upgrade.

Upgrade Firmware

As new versions of the UAP firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements. The AP uses a TFTP client for firmware upgrades. You can also use HTTP to perform firmware upgrades.

After you upload new firmware and the system reboots, the newly added firmware becomes the primary image. If the upgrade fails, the original firmware remains as the primary image.

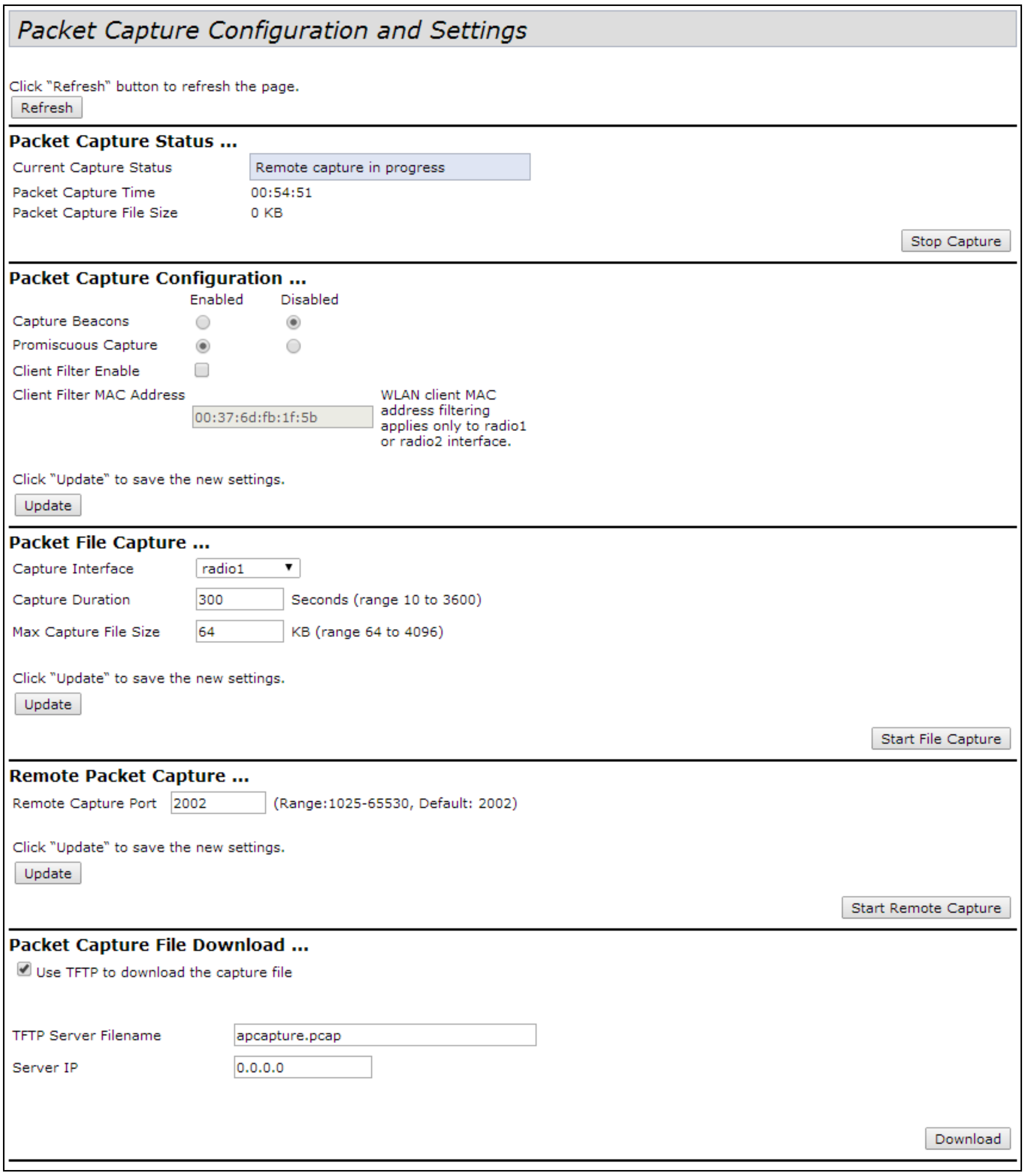
8.3 «Packet Capture» submenu

Wireless packet capture operates in two modes:

- Capture file mode
- Remote capture mode

For capture file mode, captured packets are stored in a file on the Access Point. The AP 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.

For remote capture mode, the captured packets are redirected in real time to an external PC running the Wireshark®tool.



Packet Capture Configuration and Settings

Click "Refresh" button to refresh the page.

Packet Capture Status ...

Current Capture Status	Remote capture in progress
Packet Capture Time	00:54:51
Packet Capture File Size	0 KB

Packet Capture Configuration ...

	Enabled	Disabled
Capture Beacons	○	●
Promiscuous Capture	●	○
Client Filter Enable	□	
Client Filter MAC Address	00:37:6d:fb:1f:5b	WLAN client MAC address filtering applies only to radio1 or radio2 interface.

Click "Update" to save the new settings.

Packet File Capture ...

Capture Interface	radio1 ▼	
Capture Duration	300	Seconds (range 10 to 3600)
Max Capture File Size	64	KB (range 64 to 4096)

Click "Update" to save the new settings.

Remote Packet Capture ...

Remote Capture Port 2002 (Range:1025-65530, Default: 2002)

Click "Update" to save the new settings.

Packet Capture File Download ...

☑ Use TFTP to download the capture file

TFTP Server Filename	apcapture.pcap
Server IP	0.0.0.0

Click **Refresh** button to refresh the page.

Packet Capture Status allows you to view the status of packet capture on the AP.

Field	***Description***
Current Capture Status	Shows whether packet capture is running or stopped.
Packet Capture Time	Shows elapsed capture time.
Packet Capture File Size	Shows the current capture file size.

Packet Capture Configuration allows you to configure parameters that affect how packet capture functions on the radio interfaces.

Field	***Description***
Capture Beacons	**Enable** to capture the 802.11 beacons detected or transmitted by the radio.
Promiscuous Capture	**Enable** to place the radio in promiscuous mode when the capture is active. In promiscuous mode the radio receives all traffic on the channel, including traffic that is not destined to this AP. 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 capture is completed, the radio reverts to non-promiscuous mode operation.
Client Filter Enable	**Enable** to use the WLAN client filter to capture 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:** The MAC filter is active only when capture is performed on an 802.11interface.

Click **Update** to save the new settings.

In Packet File Capture mode the AP stores captured packets in the RAM file system.

Field	***Description***
Capture Interface	Select an AP **Capture Interface** name from the drop-down menu. AP capture interface names are eligible for packet capture are: **radio1.**802.11 traffic on the radio interface Radio 1. **radio2.**802.11 traffic on Radio 2. **eth0.**802.3 traffic on the Ethernet port. **wlan0.**VAP0 traffic on Radio 1. **wlan1.**VAP0 traffic on Radio 2. **wlan0vap1 to wlan0vap7.**Traffic on the specified VAP on Radio 1. **wlan1vap1 to wlan1vap 7.**Traffic on the specified VAP on Radio 2. **wlan0wds0 to wlan0wds3.**Traffic on the specified WDS interface. **brtrunk.**Linux bridge interface in the WAP device.
Capture Duration	Specify the time duration in seconds for the capture (range 10 to 3600).
Max Capture File Size	Specify the maximum allowed size for the capture file in KB (range 64 to 4096).

Remote Packet Capture allows 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 capture server runs on the AP and sends the captured packets via a TCP connection to the Wireshark tool.

A Windows PC running the Wireshark tool allows you to display, log, and analyze captured traffic.
When the remote capture mode is in use, the AP doesn't store any captured data locally in its file system.

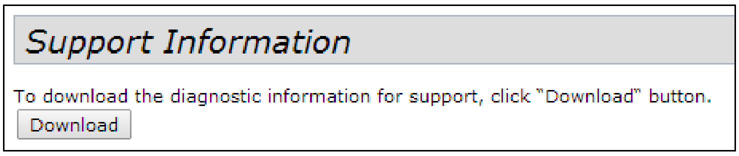
Packet Capture File Download allows you to download the capture file by TFTP to a configured TFTP server or by HTTP(S) to a PC. The captured packets are stored in file /tmp/apcapture.pcap on the AP. A capture is automatically stopped when the capture file download command is triggered.

Because the capture file is located in the RAM file system, it disappears if the AP is reset.

Field	*Description*
Use TFTP to download the capture file	To use TFTP download, check the box that indicates TFTP download. File download using HTTP(S) may be done by clicking the Download button.
TFTP Server Filename	Enter a name (1 to 255 characters) for the capture file in the TFTP Server Filename *Field*, including the .pcap file name extension and the path to the directory where you want to save the file. File name should not contain spaces, <, >, |, \, : , (,), &, ; , #, ? , * and successive '.' .
Server IP	Enter the IP address of the TFTP server.

8.4 «Support Information» submenu

The Support Information page provides a way to gather the diagnostic/troubleshooting information about the AP beyond what is available through the Web UI.



Support Information

To download the diagnostic information for support, click "Download" button.

Field	*Description*
Download	To download the diagnostic information for support, click «Download» button.

9 МЕНЮ «WI-FI SETUP»

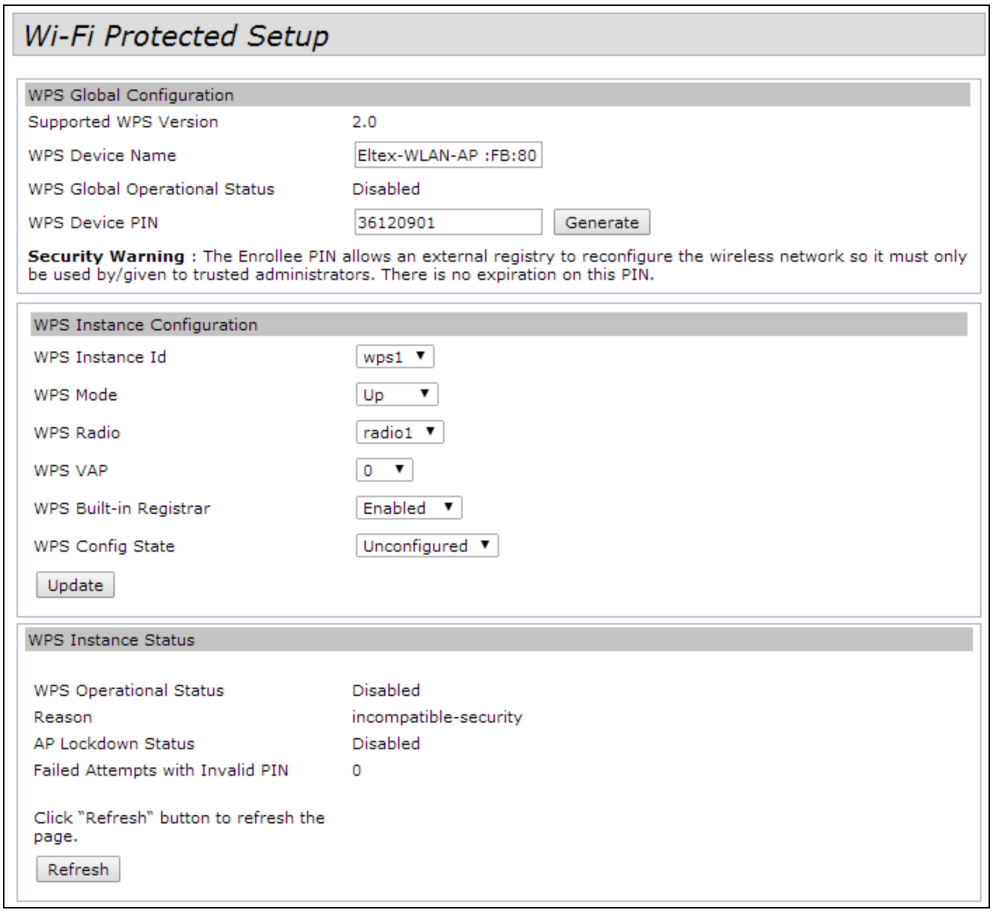
Wi-Fi Protected Setup (WPS) is a standard that enables simple establishment of wireless networks without compromising network security. It relieves both the wireless client users and the UAP administrators from having to know network names, keys, and various other cryptographic configuration options.

WPS facilitates network setup by allowing the administrator to use a push button or PIN mechanism to establish wireless networks, thereby avoiding the manual entry of network names (SSIDs) and wireless security parameters.

WPS maintains network security during these simple steps by requiring both the users of new client devices and WLAN administrators to have either physical access to their respective devices or secure remote access to these devices.

9.1 Подменю «WPS Setup»

Use the **WPS Setup** page to enable the UAP as a WPS-capable device and configure basic settings. When you are ready to use the feature to enroll a new device or add the UAP to a WPS-enabled network, use the WPS Process page.



Wi-Fi Protected Setup

WPS Global Configuration

Supported WPS Version	2.0
WPS Device Name	Eltex-WLAN-AP :FB:80
WPS Global Operational Status	Disabled
WPS Device PIN	36120901

Security Warning : The Enrollee PIN allows an external registry to reconfigure the wireless network so it must only be used by/given to trusted administrators. There is no expiration on this PIN.

WPS Instance Configuration

WPS Instance Id	wps1
WPS Mode	Up
WPS Radio	radio1
WPS VAP	0
WPS Built-in Registrar	Enabled
WPS Config State	Unconfigured

WPS Instance Status

WPS Operational Status	Disabled
Reason	incompatible-security
AP Lockdown Status	Disabled
Failed Attempts with Invalid PIN	0

Click "Refresh" button to refresh the page.

Field	*Description*
WPS Global Configuration	
Supported WPS Version	The WPS protocol version that the UAP supports.
WPS Device Name	A default device name displays. You can assign a different name of up to 32characters, including spaces and special characters.
WPS Global Operational Status	Whether the WPS protocol is enabled or disabled on the UAP. It is enabled by default.

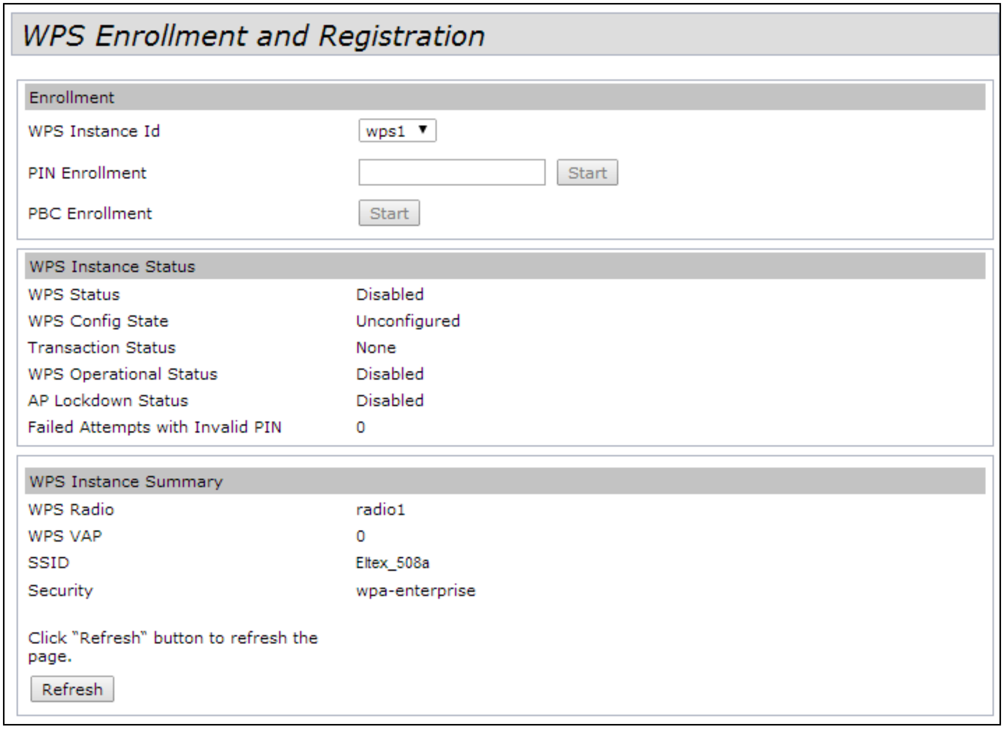
WPS Device PIN	A system-generated eight-digit WPS PIN for the UAP. The administrator may use this generated PIN to register the UAP with an external registrar. You can click **Generate** to generate a new PIN. This is advisable if network integrity has been compromised.
WPS Instance Configuration	
WPS Instance ID	An identifier for the instance. As there is only one instance, the only option iswps1.
WPS Mode	Enables or disables the instance.
WPS Radio	On a dual-radio AP, this *Field* identifies the radio associated with the instance.
WPS VAP	The VAP associated with this WPS instance.
WPS Built-in Registrar	Select to enable the built-in registrar function. When enabled, enrollees (typically WLAN clients) can register with the UAP. When disabled, the registrar functionality in the UAP is turned off and the enrollee needs to register with another registrar on the network. In this case, another device on the network acts as the registrar and the UAP serves as a proxy for forwarding client registration requests and the registrar's responses.
WPS Config State	Determines whether the VAP will be configured from the external registrar as a part of WPS process. It can be set to one of these values: • Unconfigured—VAP settings will be configured using WPS, after which the state will be change to Configured. • Configured—VAP settings will not be configured by the external registrar and will retain the existing configuration.
WPS Instance Status	
WPS Operational Status	Indicates whether or not the WPS instance is operational.
Reason	Provides additional information about the WPS operational status. If the status is*Ready*, the reason is OK. Otherwise, the reason for the status can be one of the following: • WPS disabled on radio; • VAP disabled; • SSID not set for broadcast; • Incompatible VAP security configuration; • MAC filtering enabled.
AP Lockdown Status	Indicates whether the AP is in lockdown mode, in which external registrars are blocked from registering with the AP. When in lockdown status, this *Field* reports the start time of the lockdown,whether it is temporary or permanent and, if temporary, the duration of the lockdown period. When not in lockdown mode, the status is *Disabled*.
AP PIN Failed Attempts	The number of times an external registrar has tried and failed to register with the AP.

Use the buttons to perform the following tasks:

- **Generate**: Generate a new WPS device PIN. This is advisable if network integrity has been compromised.
- **Update**: Apply and save the changes to the WPS interface configuration settings.
- **Refresh**: Refresh the page to view the current information.

9.2 «WPS Process» submenu

Use the **WPS Process** page to use the Wi-Fi Protected Setup feature to enroll a client station on the network. You can enroll a client using a pin or using the push button method, if supported on the client station.



WPS Enrollment and Registration

Enrollment

WPS Instance Id	wps1 ▼
PIN Enrollment	Start
PBC Enrollment	Start

WPS Instance Status

WPS Status	Disabled
WPS Config State	Unconfigured
Transaction Status	None
WPS Operational Status	Disabled
AP Lockdown Status	Disabled
Failed Attempts with Invalid PIN	0

WPS Instance Summary

WPS Radio	radio1
WPS VAP	0
SSID	Eltex_508a
Security	wpa-enterprise

Click "Refresh" button to refresh the page.

Field	*Description*
Enrollment	
WPS Instance ID	An identifier for the instance. The AP supports only one instance, so the only option is wps1.
PIN Enrollment	Specify the client's PIN to enroll a client by using the PIN method. Obtain the PIN from the client device. The PIN may be printed on the hardware itself, or may be obtained from the device's software interface. Click **Start** to begin the PIN method enrolment for the client. Within two minutes, enter the UAP's pin on the client station's software interface. The UAP's pin is configured on the **WPS Setup** page. When the client is enrolled, either the UAP's built-in registrar or the external registrar on the network proceeds to configure the client with the SSID, encryption mode, and public shared key of a WPS-enabled BSS. **Note:** This enrollment sequence may also work in reverse; that is, you may beable to initiate the process on the client station by entering the UAP's pin. However, this method is not recommended for security reasons, as it enables the client to configure the SSID and security settings on the AP. The administrator should share the PIN only with trusted devices.
PBC Enrollment	To begin the process of enrolling a client by using the push button method, click**Start**. Then, push the hardware button on the client station. **Note:** You can alternatively initiate this process on the client station, and then click the PBC Enrollment Start button on the UAP. When you push the button on the client station, the WPS Operational Statuschanges to Adding Enrollee. When the enrollment process is complete, the WPS Operational Status changes to Ready and the Transaction Status changes to

	Success. When the client is enrolled, either the UAP’s built-in registrar or the external registrar on the network proceeds to configure the client with the SSID, encryption mode, and public shared key of a WPS-enabled BSS.
WPS Instance Status	
WPS Status	Shows whether the WPS Setup feature is currently operational.
WPS Config State	Indicates how the SSID and Security settings will be configured on the enrollee. • Unconfigured—the SSID and Security values are configured by the externalregistrar. • Configured—the SSID and Security values are configured by the administrator.
Transaction Status	The status of the client enrollment process: • None-No client has successfully enrolled since the AP has been reset. • Success-The client successfully enrolled. • WPS Message Error-An error was encountered during the message exchange between the AP and the client being enrolled. • Timed Out-The client was unable to enroll in the allowed amount of time.
WPS Operational Status	The status of the current transaction or previous transaction. This *Field* displaysone of the following statuses: • Ready-The AP has not handled any WPS transactions handled since WPS was enabled on the VAP. • Adding Enrollee-The PIN or PCB enrollment process has been initiated. • Disabled-The WPS Setup feature is not operational. • Configuring-The enrollee is being configured. • Proxying-The WPS feature is serving as a proxy for the external registrar.
AP Lockdown Status	Indicates whether the AP is in lockdown mode, in which external registrars areblocked from registering with the AP. When in lockdown status, this *Field* reports the start time of the lockdown, whether it is temporary or permanent and, if temporary, the duration of the lockdown period. When not in lockdown mode, the status is *Disabled*.
AP PIN Failed Attempts	The number of times an external registrar has tried and failed to register with the AP.
WPS Instance Summary	
WPS Radio	On a dual-radio AP, this *Field* identifies the radio associated with the instance.
WPS VAP	The VAP associated with this WPS instance.
SSID	The SSID configured on the VAP associated with the WPS instance.
Security	The security method configured for the VAP associated with the WPS instance.
Shared Key (WPA-Personal Only)	If the security for the VAP is WPA-Personal, this *Field* shows the configured shared key. If the security is None or WPA-Enterprise, this *Field* is not visible.

Click **Refresh** to update the screen and display the most current information.

10 «CLUSTER» MENU

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 information, such as VAP settings and QoS queue parameters.

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

- The APs use the same radio mode (for example, radio 1 uses 802.11g);
- The APs are connected on the same bridged segment;
- The APs joining the cluster have the same Cluster Name;
- Clustering mode is enabled on both APs.

«CLUSTER» menu describes operation and device in the cluster mode. Claster mode allows you to adjust only one access point (wizard) in the network. Other points, in case of turning on, will find the wizard in a network and copy its configuration. Hanceforth in case of introduction of modifications to the configuration for only one access points, these modifications will be applied to all points in the cluster.

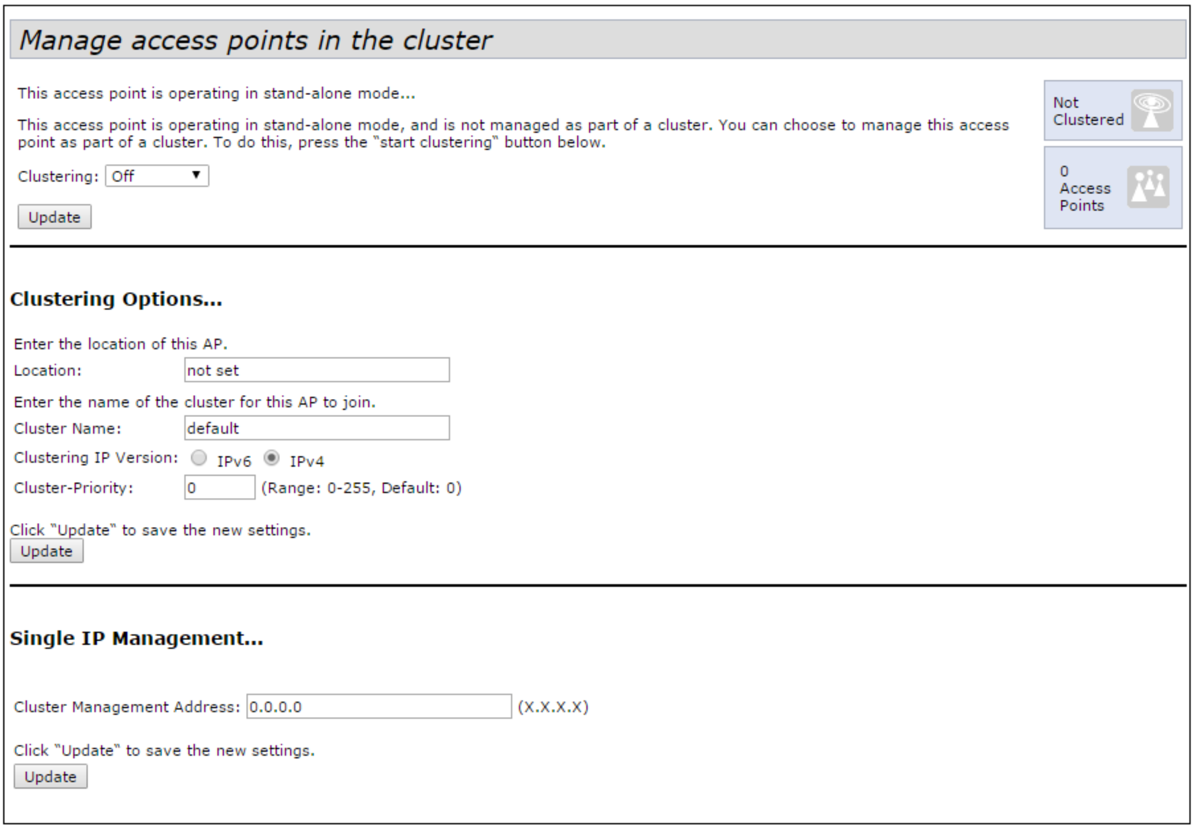
✓ **The device can operate in the cluster mode only when WDS (Wireless Distribution System) and WGB (Work Group Bridge) are turned off.**

✓ **Interface for all points must be inside the same network to work in Management Ethernet cluster**

✓ **The mode of work in cluster is turned on at the device as a default.**

10.1 «Access Points» submenu

The **Access Points** tab allows you to start or stop clustering on an AP, view the cluster members, and configure the location and cluster name for a cluster member. From the **Access Points** page, you can also click the IP address of each cluster member to navigate to configuration settings and data on an access point in the cluster.



Manage access points in the cluster

This access point is operating in stand-alone mode...

This access point is operating in stand-alone mode, and is not managed as part of a cluster. You can choose to manage this access point as part of a cluster. To do this, press the "start clustering" button below.

Clustering: Off

Clustering Options...

Enter the location of this AP.
Location: not set

Enter the name of the cluster for this AP to join.
Cluster Name: default

Clustering IP Version: ○ IPv6 ● IPv4

Cluster-Priority: 0 (Range: 0-255, Default: 0)

Click "Update" to save the new settings.

Single IP Management...

Cluster Management Address: 0.0.0.0 (X.X.X.X)

Click "Update" to save the new settings.

Field	***Description***
Clustering	If clustering is not enabled, then the AP is operating in stand-alone mode and none of the information in this table is visible. – *Clustering* – claster operation mode: ▪ *Off* – claster turn off; ▪ On – claster turn on; ▪ SoftWLC – claster operation in the mode of the compatability with SoftWLC.
Location	*Description* of where the access point is physically located.
MAC Address	Media Access Control (MAC) address of the access point. The address shown here is the MAC address for the bridge (brtrunk). This is the address by which the AP is known externally to other networks.
IP Address	Specifies the IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.
Cluster-Priority	This is supported only for ipv4. Specifies the Priority of the member access point. Configurable by user. The higher number indicates the higher preference for this AP to become the dominant AP.In case of tie, lowest MAC address becomes dominant. Range: 0 to 255. Default value is 0.
Cluster-Controller	This is supported only for ipv4. Specifies which member access point is «Dominant». If cluster member is dominant then cluster contoller *Field* shows «yes» if not it will display «no» in the table.

The following table describes the cluster information to configure for an individual member. The clustering options are read-only when clustering is enabled. To configure the clustering options, you must stop clustering.

The following table describes the cluster information to configure for an individual member. The clustering options are read-only when clustering is enabled. To configure the clustering options, you must stop clustering.

Field	Description
Location	Enter a *Description* of where the access point is physically located.
Cluster Name	Enter the name of the cluster for the AP to join. The cluster name is not sent to other APs in the cluster. You must configure the same cluster name on each AP that is a member of the cluster. The cluster name must be unique for each cluster you configure on the network.
Clustering IP Version	Specify the IP version that the APs in the cluster use to communicate with each other.
Cluster-Priority	This is supported only for ipv4. Specifies the Priority of the cluster member. Configurable by user.The higher number indicates the higher preference for this AP to become the dominant AP.In case of tie, lowest MAC address becomes dominant.Range: 0 to 255. Default value is 0.

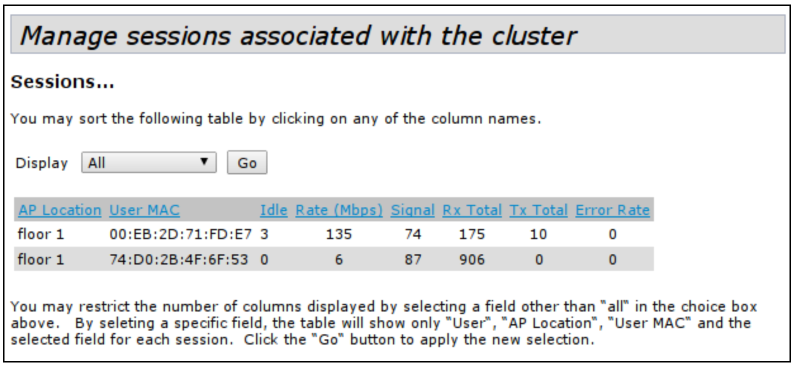
Click **Update** to save the new settings.he following table describes to configure Signgle Management.

Field	Description
Cluster Management Address	This is supported only for ipv4. In order to access the cluster with a single IP, The Cluster can be configured with an option of Cluster IP address. This is part of the global configuration of the cluster in section It has to be statically configured by the Cluster Administrator. The Cluster IP management address should be part of the same subnet as the clustered AP management IP addresses. The Cluster IP address is configured as secondary IP address to the management interface of the Dominant AP. The Dominant AP user interface is accessible using the Cluster IP address. When the Cluster IP address is set as secondary IP address on the Dominant AP, it sends Gratuitous ARPs on the management VLAN so that the mapping between the new IP address and the Mac-address is established in the subnet. The Cluster IP address configuration is shared among all the clustered APs.

10.2 «Sessions» submenu

The **Sessions** page shows information on client stations associated with access points in the cluster. Each client is identified by its MAC address, along with the AP (location) to which it is currently connected. This page shows a maximum of 20 clients per radio of the clustered APs. To see all clients associated with a particular AP, view the Status > Client Associations web page directly on that AP.

To view a particular statistic for client sessions, select an item from the Display drop-down list and click **Go**. You can view information about idle time, data rate, signal strength and so on; all of which are described in detail in the table below.



Manage sessions associated with the cluster

Sessions...

You may sort the following table by clicking on any of the column names.

Display: All ▼ Go

AP Location	User MAC	Idle	Rate (Mbps)	Signal	Rx Total	Tx Total	Error Rate
floor 1	00:EB:2D:71:FD:E7	3	135	74	175	10	0
floor 1	74:D0:2B:4F:6F:53	0	6	87	906	0	0

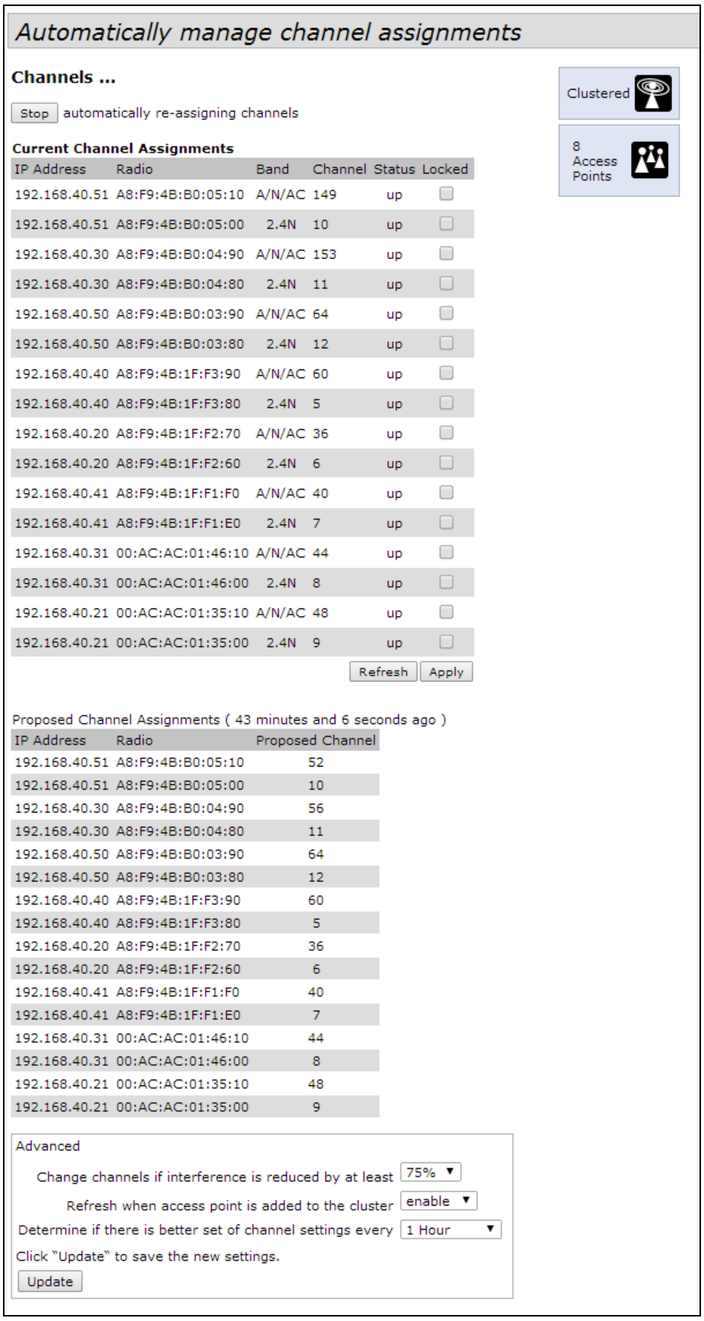
You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By seleting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

Field	*Description*
AP Location	Indicates the location of the access point. This is derived from the location *Description* specified on the **Basic Settings** tab.
User MAC	Indicates the MAC address of the wireless client device. A MAC address is a hardware address that uniquely identifies each node of a network.
Idle	Indicates the amount of time this station has remained inactive. A station is considered to be idle when it is not receiving or transmitting data.
Rate	The speed at which this access point is transferring data to the specified client. The data transmission rate is measured in *megabits per second* (Mbps). This value should fall within the range of the advertised rate set for the mode in use on the access point. For example, 6 to 54 Mbps for 802.11a.
Signal	Indicates the strength of the radio frequency (RF) signal the client receives from the access point. The measure used for this is a value known as *Received Signal Strength Indication* (RSSI), and will be a value between 0 and 100. RSSI is determined by a mechanism implemented on the network interface card (NIC) of the client station.
Receive Total	Indicates number of total packets received by the client during the current session.
Transmit Total	Indicates number of total packets transmitted to the client during this session.
Error Rate	Indicates the percentage of time frames are dropped during transmission on this access point.

10.3 «Channel Management» submenu

The Channel Management page shows previous, current, and planned channel assignments for clustered access points. By default, automatic channel assignment is disabled. You can start channel management to optimize channel usage across the cluster on a scheduled interval.

From this page, you can view channel assignments for all APs in the cluster and stop or start automatic channel management. By using the Advanced settings on the page, you can modify the interference reduction potential that triggers channel re-assignment, change the schedule for automatic updates, and re-configure the channel set used for assignments.



Automatically manage channel assignments

Channels ...

Stop automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Status	Locked
192.168.40.51	A8:F9:4B:B0:05:10	A/N/AC	149	up	☐
192.168.40.51	A8:F9:4B:B0:05:00	2.4N	10	up	☐
192.168.40.30	A8:F9:4B:B0:04:90	A/N/AC	153	up	☐
192.168.40.30	A8:F9:4B:B0:04:80	2.4N	11	up	☐
192.168.40.50	A8:F9:4B:B0:03:90	A/N/AC	64	up	☐
192.168.40.50	A8:F9:4B:B0:03:80	2.4N	12	up	☐
192.168.40.40	A8:F9:4B:1F:F3:90	A/N/AC	60	up	☐
192.168.40.40	A8:F9:4B:1F:F3:80	2.4N	5	up	☐
192.168.40.20	A8:F9:4B:1F:F2:70	A/N/AC	36	up	☐
192.168.40.20	A8:F9:4B:1F:F2:60	2.4N	6	up	☐
192.168.40.41	A8:F9:4B:1F:F1:F0	A/N/AC	40	up	☐
192.168.40.41	A8:F9:4B:1F:F1:E0	2.4N	7	up	☐
192.168.40.31	00:AC:AC:01:46:10	A/N/AC	44	up	☐
192.168.40.31	00:AC:AC:01:46:00	2.4N	8	up	☐
192.168.40.21	00:AC:AC:01:35:10	A/N/AC	48	up	☐
192.168.40.21	00:AC:AC:01:35:00	2.4N	9	up	☐

Proposed Channel Assignments (43 minutes and 6 seconds ago)

IP Address	Radio	Proposed Channel
192.168.40.51	A8:F9:4B:B0:05:10	52
192.168.40.51	A8:F9:4B:B0:05:00	10
192.168.40.30	A8:F9:4B:B0:04:90	56
192.168.40.30	A8:F9:4B:B0:04:80	11
192.168.40.50	A8:F9:4B:B0:03:90	64
192.168.40.50	A8:F9:4B:B0:03:80	12
192.168.40.40	A8:F9:4B:1F:F3:90	60
192.168.40.40	A8:F9:4B:1F:F3:80	5
192.168.40.20	A8:F9:4B:1F:F2:70	36
192.168.40.20	A8:F9:4B:1F:F2:60	6
192.168.40.41	A8:F9:4B:1F:F1:F0	40
192.168.40.41	A8:F9:4B:1F:F1:E0	7
192.168.40.31	00:AC:AC:01:46:10	44
192.168.40.31	00:AC:AC:01:46:00	8
192.168.40.21	00:AC:AC:01:35:10	48
192.168.40.21	00:AC:AC:01:35:00	9

Advanced

Change channels if interference is reduced by at least 75%

Refresh when access point is added to the cluster enable

Determine if there is better set of channel settings every 1 Hour

Click "Update" to save the new settings.

Click **Start** to resume automatic channel assignment.

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

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

The following table provides details about Current Channel Assignments.

Field	***Description***
IP Address	Specifies the IP Address for the access point.
Radio	Identifies the MAC address of the radio.
Band	Indicates the band on which the access point is broadcasting.
Current	Indicates the radio Channel on which this access point is currently broadcasting.
Locked	Click **Locked** to force the access point to remain on the current channel. When Locked is selected (enabled) for an access point, automated channel management plans will not re-assign 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. If you click **Update**, you will see that locked APs show the same channel for the Current Channel and Proposed Channel *Field*s. Locked APs will keep their current channels.

The *Proposed Channel Assignments* shows the last channel plan. The plan lists all access points in the cluster by IP Address, and shows the current and proposed channels for each AP. Locked channels will not be re-assigned and the optimization of channel distribution among APs will take into account the fact that locked APs must remain on their current channels. APs that are not locked may be assigned to different channels than they were previously using, depending on the results of the plan.

Field	***Description***
IP Address	Specifies the IP Address for the access point.
Radio	Indicates the radio channel on which this access point is currently broadcasting.
Proposed Channel	Indicates the radio channel to which this access point would be re-assigned if the Channel Plan is executed.

The Advanced settings allow you to customize and schedule the channel plan for the cluster.

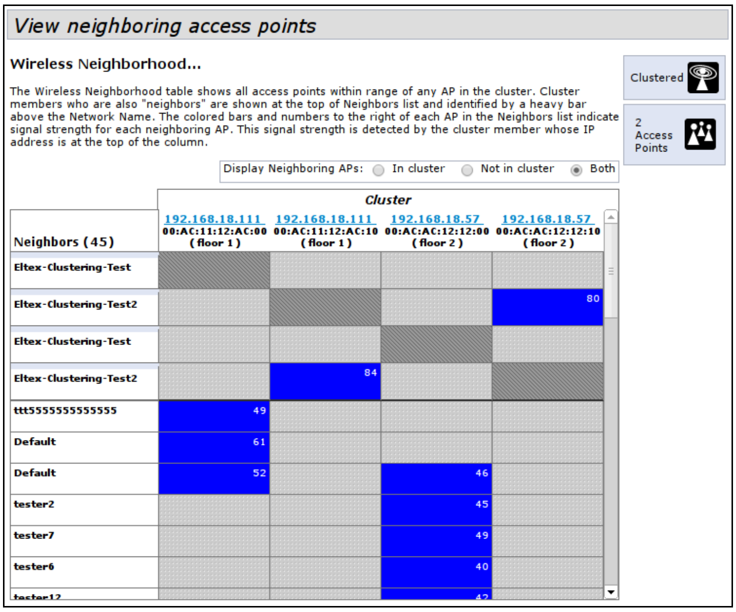
Field	***Description***
Change channels if interferenceis reduced by at least	Specify the minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is 75 percent. Use the drop-down menu to choose percentages ranging from 5 percent to 75 percent. This setting lets you set a gating factor for channel re-assignment 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 re-assigned. However; if you re-set the minimal channel interference benefit to 25 percent and click **Update**, the proposed channel plan will be implemented and channels re-assigned as needed.
Determine if there is better set ofchannels every	Use the drop-down menu to specify the schedule for automated updates. A range of intervals is provided, from 30 Minutes to 6 Months The default is 1 Hour (channel usage re-assessed and the resulting channel plan applied every hour).

Click **Update** under Advanced settings to apply these settings.

10.4 «Wireless Neighborhood» submenu

The Wireless Neighborhood shows up to 20 access points per radio within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and non-members.

For each neighbor access point, the Wireless Neighborhood view shows identifying information (SSID or Network Name, IP Address, MAC address) along with radio statistics (signal strength, channel, beacon interval). You can click on an AP to get additional statistics about the APs in radio range of the currently selected AP.



View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ○ In cluster ○ Not in cluster ● Both

	Cluster			
Neighbors (45)	192.168.18.111 00:AC:11:12:AC:00 (floor 1)	192.168.18.111 00:AC:11:12:AC:10 (floor 1)	192.168.18.57 00:AC:AC:12:12:00 (floor 2)	192.168.18.57 00:AC:AC:12:12:10 (floor 2)
Eltex-Clustering-Test	▨			
Eltex-Clustering-Test2		▨		80
Eltex-Clustering-Test			▨	
Eltex-Clustering-Test2		84		▨
ttt5555555555555	49			
Default	61			
Default	52		46	
tester2			45	
tester7			49	
tester6			40	
tester12			42	

The Wireless Neighborhood view can help you:

Detect and locate unexpected (or *rogue*) access points in a wireless domain so that you can take action to limit associated risks.

Verify coverage expectations. By assessing which APs are visible at what signal strength from other APs, you can verify that the deployment meets your planning goals.

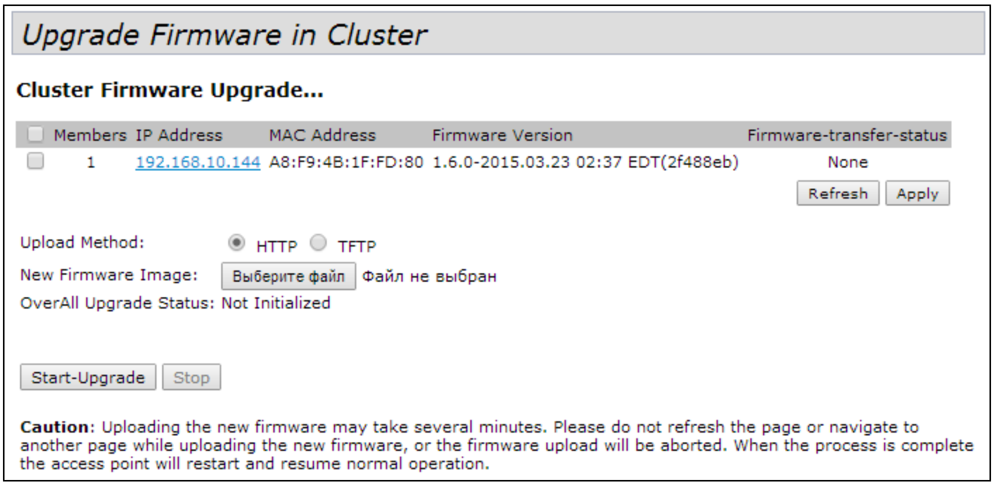
Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the color coded table.

The following table describes details about the Wireless Neighborhood information.

Field	***Description***
Display neighboring APs	Click one of the following radio buttons to change the view: • **In cluster**-Shows only neighbor APs that are members of the cluster • **Not in cluster**-Shows only neighbor APs that are not cluster members • **Both**-Shows all neighbor APs (cluster members and non-members)

10.5 «Cluster Firmware Upgrade» submenu

Cluster provides a centralized cluster firmware upgrade feature that allows all the APs in the cluster to be upgraded from the Dominant AP. The Cluster firmware upgrade can be performed only from the dominant AP. For each member access point, the cluster firmware upgrade page shows identifying information (All members checkboxor selective members checkbox, IP Address, Firmare Version and Firmware transfer status).



Upgrade Firmware in Cluster

Cluster Firmware Upgrade...

□ Members	IP Address	MAC Address	Firmware Version	Firmware-transfer-status
□ 1	192.168.10.144	A8:F9:4B:1F:FD:80	1.6.0-2015.03.23 02:37 EDT(2f488eb)	None

Upload Method: ● HTTP ○ TFTP

New Firmware Image: Выберите файл Файл не выбран

OverAll Upgrade Status: Not Initialized

Caution: Uploading the new firmware may take several minutes. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the process is complete the access point will restart and resume normal operation.

The following table explains the details shown about the selected AP and other *Field*s of Cluster Firmware upgrade page.

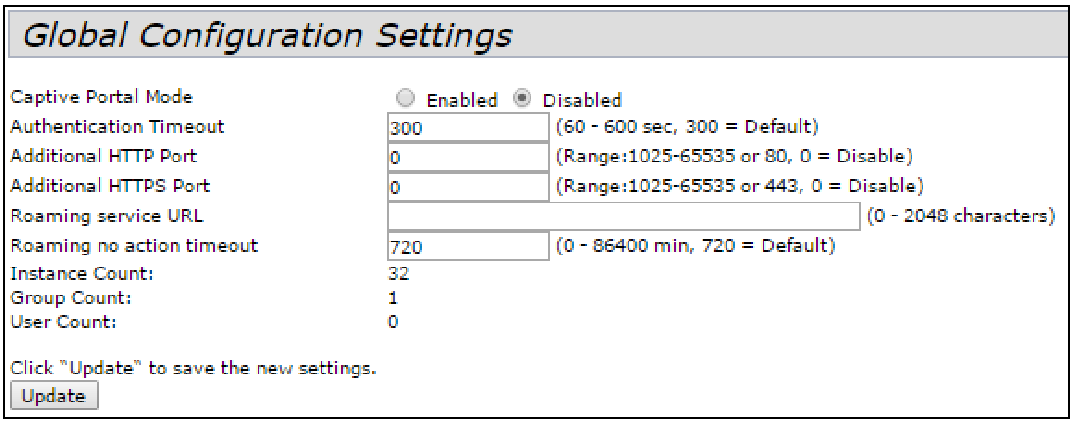
Field	*Description*
Members	The *Members Field displays* (cluster member)access points. The total supported cluster members are 10.
IP Address	Shows the IP address of the member access points.
MAC Address	Shows the MAC address of the member access points.
Firmware Version	Shows current running firmware version of the cluster member.
Firmware-transfer-status	Shows whether the firmware download and validation in cluster member is successful or failure (None/Started/Donwloaded/Success/Fail/Abort_admin/Abort_local/Dap_resigned).
Firmware-transfer-progress-bar	Shows the progress bar for firmware download. This *Field* will be displayed only when firmware download is in progress to non-dominant members.
Upload Method	Administrator planning to use centralized cluster firmware must provide a TFTP or HTTP/HTTPS mechanism for Dominant AP to download the AP image. The image is downloaded and stored in the ram disk (/tmp) of the dominant AP as a file
New Firmware Image	Show the New Firmware Image selected.
OverAll Upgrade Status	Shows the Overall upgrade status (In_progress/Completed/Fail/Abort_admin/None).
Start-Upgrade	Starts the image upgrade of all members or selectively.
Stop	Stop the Image upgrade of all members or selected members.

11 «CAPTIVE PORTAL» MENU

The Captive Portal (CP) feature allows you to block wireless clients from accessing the network until user verification has been established.

11.1 Подменю «Global Configuration»

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



Global Configuration Settings

Captive Portal Mode	○ Enabled ● Disabled	
Authentication Timeout	300	(60 - 600 sec, 300 = Default)
Additional HTTP Port	0	(Range:1025-65535 or 80, 0 = Disable)
Additional HTTPS Port	0	(Range:1025-65535 or 443, 0 = Disable)
Roaming service URL		(0 - 2048 characters)
Roaming no action timeout	720	(0 - 86400 min, 720 = Default)
Instance Count:	32	
Group Count:	1	
User Count:	0	

Click "Update" to save the new settings.

The following table describes the *Fields* on the CP **Global Configuration** page.

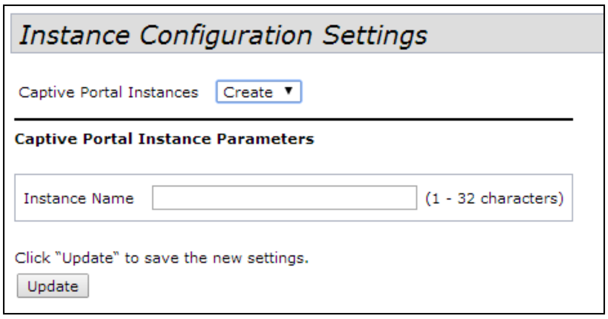
Field	*Description*
Captive Portal Mode	Enables or disables the administrative mode of CP on the AP.
Authentication Timeout	To access the network through a portal, the client must first enter authentication information on an authentication Web page. This *Field* specifies the number of seconds the AP keeps a CP authentication session open with the associated wireless client. Client CP session is disconnected if the client does not open authentication WEB page and enter valid credentials within the configured number of seconds. The CP association request will be initiated again if the client still sends the CP data traffic. The default authentication timeout is 300 seconds.
Additional HTTP Port	HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 1025-65535. Port number 80 or 443 cannot be used, and the HTTP and HTTPs ports cannot be the same.
Additional HTTPS Port	HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 1025-65535. Port number 80 or 443 cannot be used, and the HTTP and HTTPs ports cannot be the same.
Instance Count	The number of CP instances currently configured on the AP. Up to two instances can be configured.
Group Count	The number of CP groups currently configured on the AP Up to two groups can be configured. Default Group exists by default and cannot be deleted.
User Count	The number of CP users currently configured on the AP. Up to 128 users can be configured.

Click **Update** to save the new settings.

11.2 «Instance Configuration» submenu

You can create up to two Captive Portal instances; each CP instance is a defined set of instance parameters. Instances can be associated with one or more VAPs. Different instances can be configured to respond differently to users as they attempt to access the associated VAP.

The following table describes the *Field*s on the CP **Instance Configuration** page. The *Field*s that appear on the page depend on the option selected from the **Captive Portal Instances** menu.



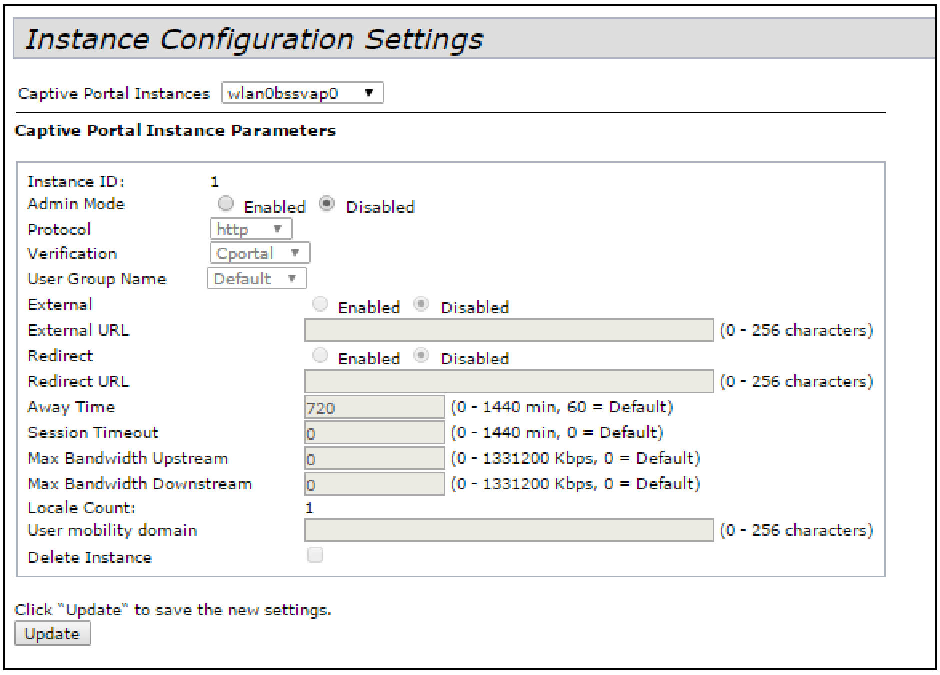
Instance Configuration Settings

Captive Portal Instances: Create

Captive Portal Instance Parameters

Instance Name: (1 - 32 characters)

Click "Update" to save the new settings.



Instance Configuration Settings

Captive Portal Instances: wlan0bssvap0

Captive Portal Instance Parameters

Instance ID:	1	
Admin Mode	○ Enabled ● Disabled	
Protocol	http	
Verification	Cportal	
User Group Name	Default	
External	○ Enabled ● Disabled	
External URL		(0 - 256 characters)
Redirect	○ Enabled ● Disabled	
Redirect URL		(0 - 256 characters)
Away Time	720	(0 - 1440 min, 60 = Default)
Session Timeout	0	(0 - 1440 min, 0 = Default)
Max Bandwidth Upstream	0	(0 - 1331200 Kbps, 0 = Default)
Max Bandwidth Downstream	0	(0 - 1331200 Kbps, 0 = Default)
Locale Count:	1	
User mobility domain		(0 - 256 characters)
Delete Instance	□	

Click "Update" to save the new settings.

Field	***Description***
Captive Portal Instances	Select an existing instance to view or configure its settings, or select **Create** to configure a new CP instance. The UAP supports two instances. If both instances have been configured, you must delete an instance before you can create a new one.
Instance Name	This *Field* is available only if **Create** is selected from the **Captive Portal Instances** *Field*. Specify a name for the new CP instance.
Instance ID	The CP instance identifier. For an existing instance, this *Field* cannot be configured. When creating a new CP instance, the ID cannot be used by another CP instance. If you attempt to assign an Instance ID that is in use, an error message is displayed.
Admin Mode	Select the option to enable the administrative mode of the selected CP instance, or clear the option to disable it.
Protocol	Specifies HTTP or HTTPs as the protocol for the CP instance to use during the verification process.

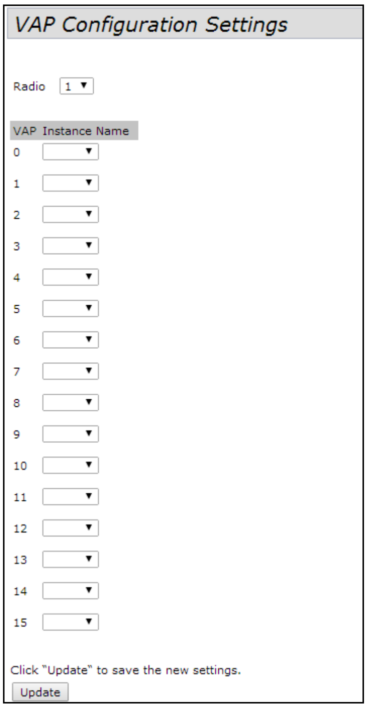
Verification	The authentication method for CP to use to verify clients:
Redirect	Specifies that CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.
Redirect URL	Enter the URL, either IPv4 or an IPv6 address, to which the newly authenticated client is redirected if the URL Redirect Mode is enabled. The IPv4 address should be in a form similar to http://xxx.xxx.xxx.xxx (http://192.0.2.10). The IPv6 address should be in a form similar to http://[xxxx:xxxx:xxxx:xxxx::xxxx:xxxx:xxxx:xxxx] (http://[2001:DB8::CAD5:7D91])
Away Time	The amount of time a user remains in the CP authenticated client list after it disassociates from the AP. If the time specified in this *Field* expires before the client attempts to reauthenticate, its entry is removed from the authenticated client list. The range is from 0 to 1440 minutes. The default value is 60 minutes. **Note:** An away timeout value is also configured for each user. See the **Local Users** page. The user’s away timeout value has precedence over the value configured here.
Session Timeout	The amount of time to wait before terminating a session. A user is logged out after the session timeout is reached. If the value is set to 0, the timeout is not enforced. The range is from 0 to 1440 minutes. The default value is 0.
Max Bandwidth Upstream	The maximum upload speed, in megabits per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network. The range is from 0 to 300 Mbps. The default value is 0.
Max Bandwidth Downstream	The maximum download speed, in megabits per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network. The range is from 0 to 300 Mbps. The default value is 0.
User Group Name	The user group associated with this instance. Each CP user is associated with a group, and a group is associated with a CP instance.
Global RADIUS	If the Verification Mode is RADIUS, select to specify that the default Global RADIUS server list is used to authenticating clients. If you want the CP feature to use a different set of RADIUS servers, clear this setting and configure the servers in the *Field*s on this page.
RADIUS Accounting	Enables tracking and measuring the resources a particular user has consumed, such as system time and amount of data transmitted and received. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers, and for globally or locally configured servers.
RADIUS IP Network	Specify whether the RADIUS IP addresses are IPv4 or IPv6 RADIUS server addresses.
RADIUS IP	The IPv4 or IPv6 address for the primary RADIUS server for this VAP. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10). The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91). When the first wireless client tries to authenticate with a VAP, the UAP sends an authentication request to the primary server. If the primary server responds to the authentication request, the UAP continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify.
RADIUS Backup IP 1-3	Up to three IPv4 or IPv6 backup RADIUS server addresses. If authentication fails with the primary server, each configured backup server is tried in sequence.
RADIUS Current	Specify which RADIUS server to use to authenticate clients:
RADIUS Key	The shared secret key that the UAP uses to authenticate to the

	primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text you enter will be displayed as «*» characters.
RADIUS Backup Key 1-3	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.
Locale Count	The number of locales associated with the instance. You can create and assign up to three different locales to each CP instance from the Web Customization page.
Delete Instance	To delete the current instance, select this option and click **Update**.

Click **Update** to save the new settings.

11.3 «VAP Configuration» submenu

Use the **Instance Association** page to associate a CP instance to a VAP. The associated CP instance settings will apply to users who attempt to authenticate on the VAP.



Click "Update" to save the new settings.

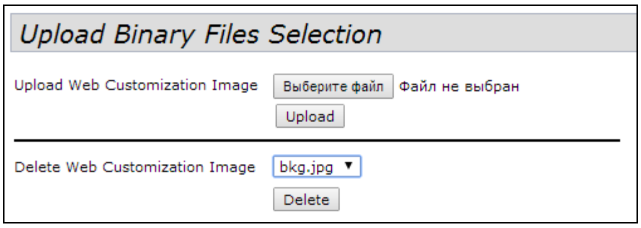
The following table describes the *Field*s on the CP **VAP Configuration** page.

Field	***Description***
RADIO	Select the radio associated with the VAP to configure.
VAP	The list of VAP IDs. A CP instance can be associated with multiple VAPs.
Instance Name	Select the instance to associate with each VAP. If the menu is blank, no instance is associated with the VAP.

Click **Update** to save the new settings.

11.4 «Upload Binary Files» submenu

When users initiate access to a VAP that is associated to a captive portal instance, an authentication page displays. You can customize this page with your own logo and other graphics.



Upload Binary Files Selection

Upload Web Customization Image: Выберите файл Файл не выбран

Upload

Delete Web Customization Image: bkg.jpg

Delete

Up to 18 images can be uploaded (assuming six locales, with each locale having three images).

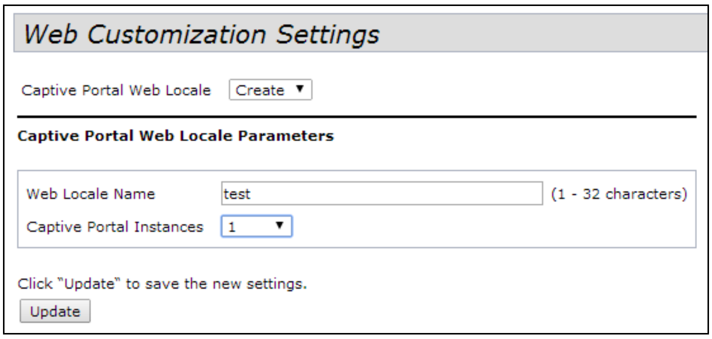
Images will be resized to fit the specified dimensions. For best results, the logo and account images should be similar in proportion to the default images, as follows:

Image Type	*Use*	*Default Width x Height*
Background	Displays in the page background.	10 × 800 pixels
Logo	Displays at top left of page to provide branding information.	168 × 78 pixels
Account	Displays above the login *Field* to depict an authenticated login.	295 × 55 pixels

To remove an image that has been uploaded, select the name of the image from the available menu and click **Delete**.

11.5 «Web Customization» submenu

When users initiate access to a VAP that is associated with a captive portal instance, an authentication page displays. You can use the page to create unique pages for different locales on your network, and to customize the textual and graphic elements of the pages. Use this page to create and customize the authentication page.



Web Customization Settings

Captive Portal Web Locale: Create

Captive Portal Web Locale Parameters

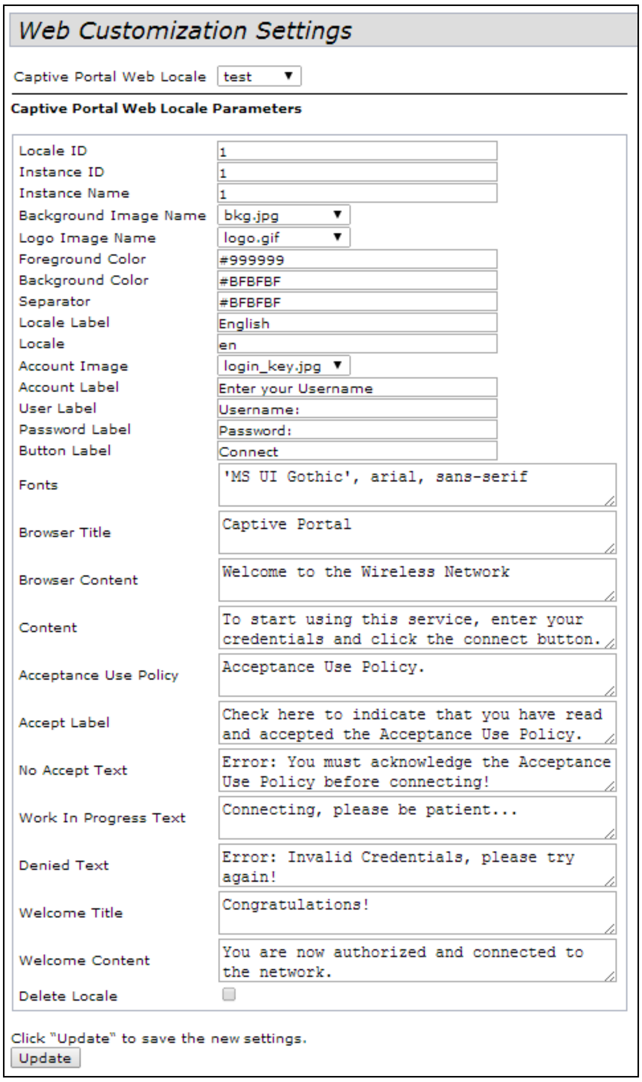
Web Locale Name: test (1 - 32 characters)

Captive Portal Instances: 1

Click "Update" to save the new settings.

Update

To create a new Web locale, select **Create** from the available menu. To view or update an existing Web locale, select its name from the menu. Click **Update** to save the new settings.



Web Customization Settings

Captive Portal Web Locale: test ▼

Captive Portal Web Locale Parameters

Locale ID	1
Instance ID	1
Instance Name	1
Background Image Name	bkg.jpg ▼
Logo Image Name	logo.gif ▼
Foreground Color	#999999
Background Color	#BFBFBF
Separator	#BFBFBF
Locale Label	English
Locale	en
Account Image	login_key.jpg ▼
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 and click the connect button.
Acceptance Use Policy	Acceptance Use Policy.
Accept Label	Check here to indicate that you have read and accepted the Acceptance Use Policy.
No Accept Text	Error: You must acknowledge the Acceptance Use Policy before connecting!
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 to the network.
Delete Locale	□

Click "Update" to save the new settings.

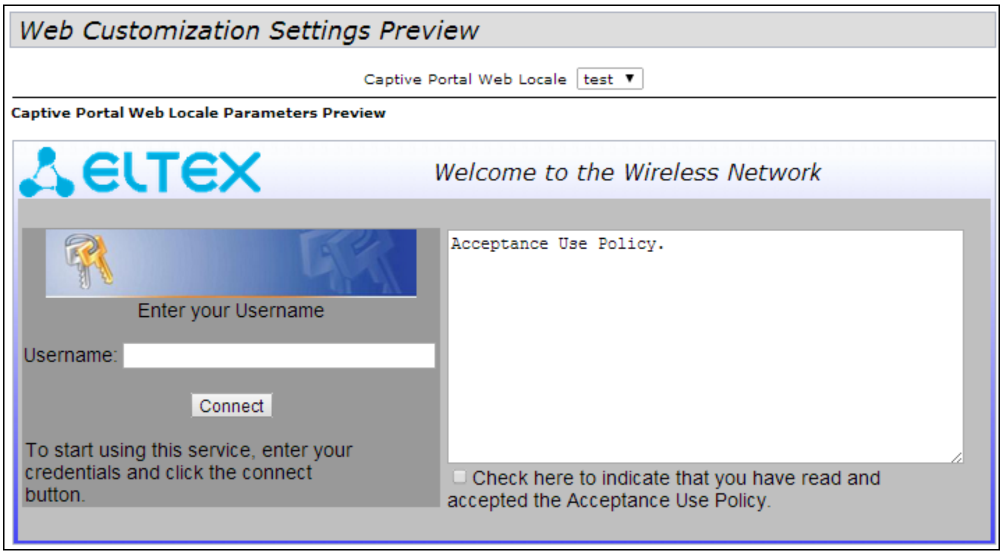
Field	Description
Locale ID	The ID that is automatically assigned o the locale when it is created. The IDcannot be configured.
Instance ID	The ID of the CP instance associated with the locale.
Instance Name	The user-configured name of the CP instance.
Background Image Name	The image to display as the page background. You can click Upload/DeleteCustom Image to upload images to the AP for use with Captive Portal instances.
Logo Image Name	The image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo. If you uploaded a custom logo image to the UAP, you can select it from the list.
Foreground color	The HTML code for the foreground color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #999999.
Background color	The HTML code for the background color in 6-digit hexadecimal format. Therange is from 1 to 32 characters. The default is #BFBFBF.
Separator	The HTML code for the color of the thick horizontal line that separates the page header from the page body, in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #BFBFBF. The default is #BFBFBF.
Locale Label	A descriptive label for the locale, from 1 to 32 characters. The default is English.
Locale	An abbreviation for the locale, from 1 to 32 characters. The default is en.

Account Image	The image file to display above the login *Field* to depict an authenticated login.
Account Label	The text that instructs the user to enter a user name. The range is from 0 to 32 characters.
User Label	The label for the user name text box. The range is from 0 to 32 characters.
Password Label	The label for the user password text box. The range is from 0 to 64 characters.
Button Label	The label on the button users click to submit their user name/password forauthentication. 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 CP page. You can enter multiplefont names, each separated by a comma. If the first font is not available on the client system, the next font will be used, and so on. For font names that have spaces, surround the entire name in quotes. The range is from 1 to 512 characters. The default is MS UI Gothic, Arial, sans-serif.
Browser Title	The text to display in the browser title bar. The range is from 1 to 128 characters. The default is Captive Portal.
Browser Content	The text that displays in the page header, to the right of the logo. The range is from 1 to 128 characters. The default is Welcome to the Wireless Network.
Content	The instructive text that displays in the page body below the user name andpassword text boxes. The range is from 0 to 256 characters. The default is: To start using this service, enter your credentials and click the connect button.
Acceptance Use Policy	The text that appears in the Acceptance Use Policy box. The range is from 0 to 8192 characters. The default is: Acceptance Use Policy.
Accept Label	The text that instructs users to select the check box to acknowledge reading and accepting the Acceptance Use Policy. The range is from 0 to 128 characters. The default is: Check here to indicate that you have read and accepted the Acceptance Use Policy.
No Accept Text	The text that displays in a pop-up window when a user submits login credentials without selecting the Acceptance Use Policy check box. The range is from 1 to 128 characters. The default is: Error: You must acknowledge the Acceptance Use Policy before connecting!
Work In Progress Text	The text that displays during authentication. The range is from 1 to 128characters. The default is: Connecting, please be patient....
Denied Text	The text that displays when a user fails authentication. The range is from 1 to128 characters. The default is: Error: Invalid Credentials, please try again!
Welcome Title	The text that displays when the client has authenticated to the VAP. The range is from 1 to 128 characters. The default is: Congratulations!
Welcome Content	The text that displays when the client has connected to the network. The range is from 0 to 256 characters. The default is: You are now authorized and connected to the network.
Delete Locale	To delete the current locale, select this option and click **Update**.

11.6 «Web Customization Preview» submenu

Use the **Web Customization Preview** page to view an example of the authentication page a CP user sees upon connecting to the UAP.

To preview a CP authentication page, select the Web locale from the menu.



Web Customization Settings Preview

Captive Portal Web Locale: test

Captive Portal Web Locale Parameters Preview

Welcome to the Wireless Network

Enter your Username

Username:

Connect

To start using this service, enter your credentials and click the connect button.

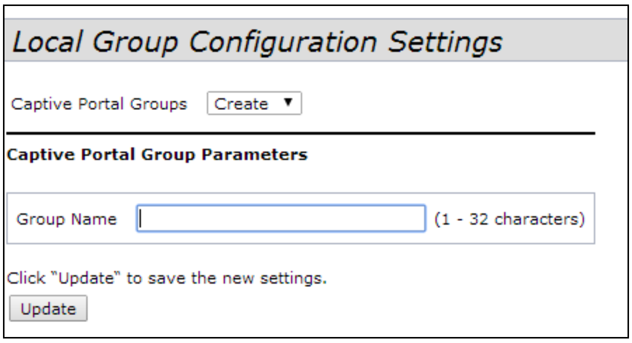
Acceptance Use Policy.

□ Check here to indicate that you have read and accepted the Acceptance Use Policy.

11.7 «Local Groups» submenu

Each local user is assigned to a user group. Each group is assigned to a CP instance. The group facilitates managing the assignment of users to CP instances.

The user group named Default is built-in and cannot be deleted. You can create up to two additional user groups. The *Field*s available on the page depend on the option selected from the Captive Portal Groups menu.



Local Group Configuration Settings

Captive Portal Groups: Create

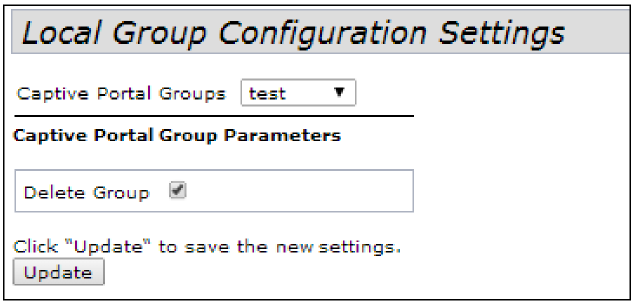
Captive Portal Group Parameters

Group Name: (1 - 32 characters)

Click "Update" to save the new settings.

Update

The menu includes all CP groups that exist on the switch. To create a new group, select **Create**. To delete a CP group, select the group name. Click **Update** to save the new settings. This *Field* is available only if the option selected from the Captive Portal Groupmenu is **Create**. Specify a name for the local user.



Local Group Configuration Settings

Captive Portal Groups: test

Captive Portal Group Parameters

Delete Group ☑

Click "Update" to save the new settings.

Update

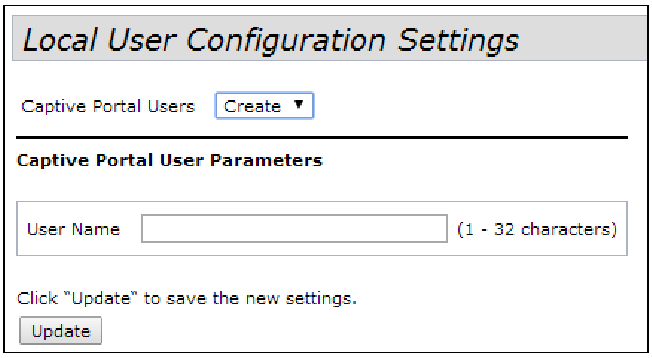
This *Field* is available only if the option selected from the Captive Portal Groupmenu is a user-created CP group. To delete the selected group, select the check box and click **Update**.

11.8 «Local Users» submenu

You can configure a captive portal instance to accommodate both guest users and authorized users. Guest users do not have assigned user names and passwords.

Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users are typically assigned to a CP instance that is associated with a different VAP than guest users.

Use the **Local Users** page to configure up to 128 authorized users in the local database.



Local User Configuration Settings

Captive Portal Users: Create ▼

Captive Portal User Parameters

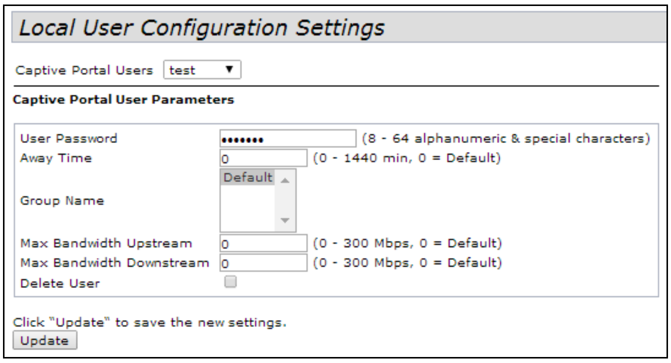
User Name: (1 - 32 characters)

Click "Update" to save the new settings.

Update

To create a new users, select **Create**. Click **Update** to save the new settings

After you create a user or select an existing user from the Captive Portal Users menu, additional *Field*s appear on the screen.



Local User Configuration Settings

Captive Portal Users: test ▼

Captive Portal User Parameters

User Password: ••••••• (8 - 64 alphanumeric & special characters)

Away Time: 0 (0 - 1440 min, 0 = Default)

Group Name: Default

Max Bandwidth Upstream: 0 (0 - 300 Mbps, 0 = Default)

Max Bandwidth Downstream: 0 (0 - 300 Mbps, 0 = Default)

Delete User: □

Click "Update" to save the new settings.

Update

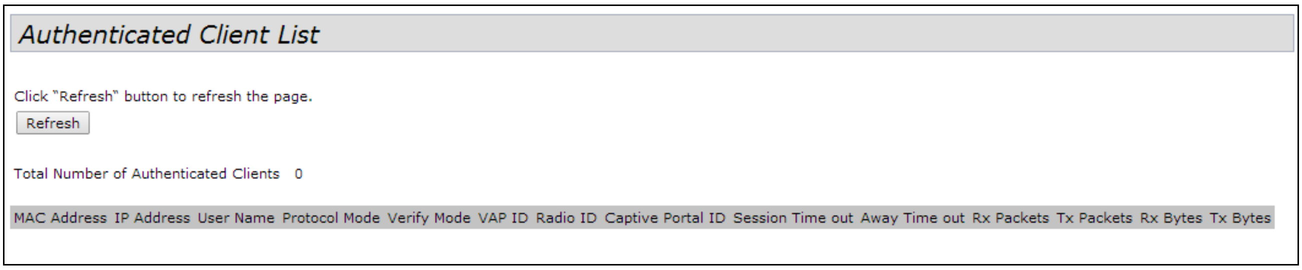
The following table describes the *Field*s on the CP **Local Users** page that you use to configure settings for an existing CP local user.

Field	***Description***
Captive Portal Users	Select the name of the user with the settings to configure.
User Password	Enter the user's password, from 8 to 64 alphanumeric and special characters. A user enter must enter the password to log into the network through the Captive Portal.
Away Time	The amount of time a user remains in the CP authenticated client list after itdisassociates from the AP. If the time specified in this *Field* expires before the client attempts to reauthenticate, its entry is removed from the authenticated client list. The range is from 0 to 1440 minutes. The default value is 0. **Note:** An away timeout value is also configured for a captive portal instance.See the **Instance Configuration** page. The timeout value configured for a local user has precedence over the value configured for the captive portal instance.
Group Name	Select the group to which the user belongs. Each CP instance is configured tosupport a particular group of users. **Note:** Each Group must contain atleast one user inorder to avoid CP authentication failures.

Maximum Bandwidth Upstream	The maximum upload speed, in megabits per second, that a client can transmit traffic when using the captive portal. This setting limits the client’s bandwidth used to send data into the network. The range is from 0 to 1331200 Kbps. The default is 0.
Maximum BandwidthDownstream	The maximum download speed, in megabits per second, that a client canreceive traffic when using the captive portal. This setting limits the client’s bandwidth used to receive data from the network. The range is from 0 to 1331200 Kbps. The default is 0.
Delete User	To delete the current user, select this option and click **Update**.

11.9 «Authenticated Clients» submenu

The **Authenticated Clients** page provides information about clients that have authenticated on any Captive Portal instance.



Authenticated Client List

Click "Refresh" button to refresh the page.

Refresh

Total Number of Authenticated Clients 0

MAC Address	IP Address	User Name	Protocol Mode	Verify Mode	VAP ID	Radio ID	Captive Portal ID	Session Time out	Away Time out	Rx Packets	Tx Packets	Rx Bytes	Tx Bytes

Click **Refresh** button to refresh the page.

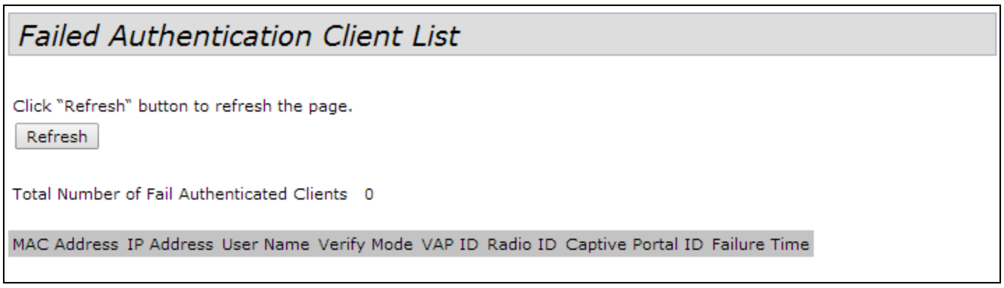
The following table describes the *Field*s on the CP **Authenticated Clients** page.

Field	***Description***
Total Number ofAuthenticated Clients	The number of clients that have successfully authenticated on any CP instance. Thisnumber includes only clients that are currently authenticated.
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 or Autoconfiguration or statically configured, will be used.
User Name	The client’s Captive Portal user name.
Protocol Mode	The protocol the user used to establish the connection (HTTP or HTTPS).
Verify Mode	The method used to authenticate the user on the Captive Portal, which can be one ofthese values:
VAP ID	The VAP that the user is associated with.
Radio ID	The ID of the radio. Because the WAP321 has a single radio, this *Field* always displaysRadio1.
Captive Portal ID	The ID of the Captive Portal instance to which the user is associated.
Session Timeout	The time remaining, in seconds, for the CP session to be valid. After the time reacheszero, the client is deauthenticated.
Away Timeout	The time remaining, in seconds, for the client to be valid. The timer starts when

	the client dissociates from the CP. After the time reaches zero, the client is deauthenticated.
Rx Packets	The number of IP packets received by the UAP from the user station.
Tx Packets	The number of IP packets transmitted from the UAP to the user station.
Rx Bytes	The number of bytes received by the UAP from the user station.
Tx Bytes	The number of bytes transmitted from the UAP to the user station.

11.10 «Failed Authentication Clients» submenu

The **Failed Authenticated Clients** page lists information about clients that attempted to authenticate on a Captive Portal and failed.



Failed Authentication Client List

Click "Refresh" button to refresh the page.

Refresh

Total Number of Fail Authenticated Clients 0

MAC Address	IP Address	User Name	Verify Mode	VAP ID	Radio ID	Captive Portal ID	Failure Time

Click **Refresh** button to refresh the page.

Field	*Description*
MAC Address	The MAC address of the client.
IP Address	The IP address of the client.
User Name	The client's Captive Portal user name.
Verify Mode	The method the client attempted to use to authenticate on the Captive Portal, which can be one of these values:
VAP ID	The VAP that the user attempted to associated with.
Radio ID	The ID of the radio that the user attempted to connect to.
Captive Portal ID	The ID of the Captive Portal instance to which the user attempted to associate.
Failure Time	The time that the authentication failure occurred. A timestamp is included that shows the time of the failure.

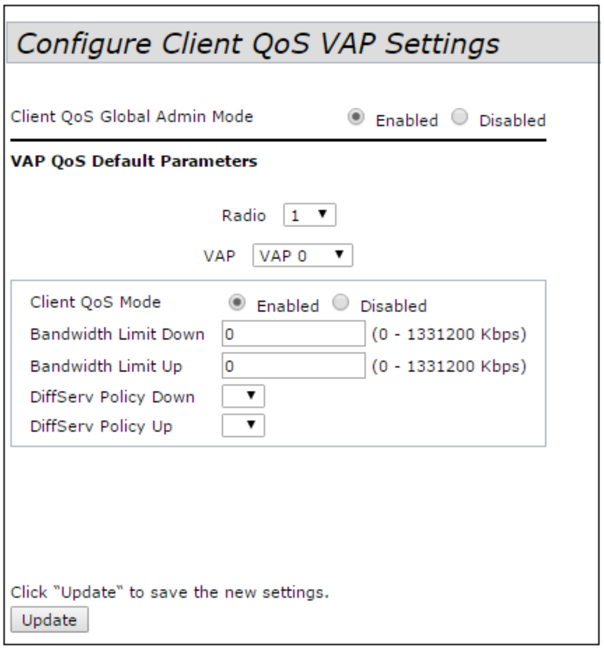
12 «CLIENT QOS» MENU

The client QoS features on the UAP provide additional control over certain QoS aspects of wireless clients that connect to the network, such as the amount of bandwidth an individual client is allowed to send and receive. To control general categories of traffic, such as HTTP traffic or traffic from a specific subnet, you can configure ACLs and assign them to one or more VAPs.

In addition to controlling general traffic categories, Client QoS allows you to configure per-client conditioning of various micro-flows through Differentiated Services (DiffServ). DiffServ policies are a useful tool for establishing general micro-flow definition and treatment characteristics that can be applied to each wireless client, both inbound and outbound, when it is authenticated on the network.

12.1 «VAP QoS Parametrs» submenu

From the **VAP QoS Parameters** page, you can enable the Client QoS feature, specify client bandwidth limits, and select the ACLs and DiffServ policies to use as default values for clients associated with the VAP when the client does not have their own attributes defined by a RADIUS server.



Configure Client QoS VAP Settings

Client QoS Global Admin Mode ● Enabled ○ Disabled

VAP QoS Default Parameters

Radio: 1

VAP: VAP 0

Client QoS Mode ● Enabled ○ Disabled

Bandwidth Limit Down: 0 (0 - 1331200 Kbps)

Bandwidth Limit Up: 0 (0 - 1331200 Kbps)

DiffServ Policy Down:

DiffServ Policy Up:

Click "Update" to save the new settings.

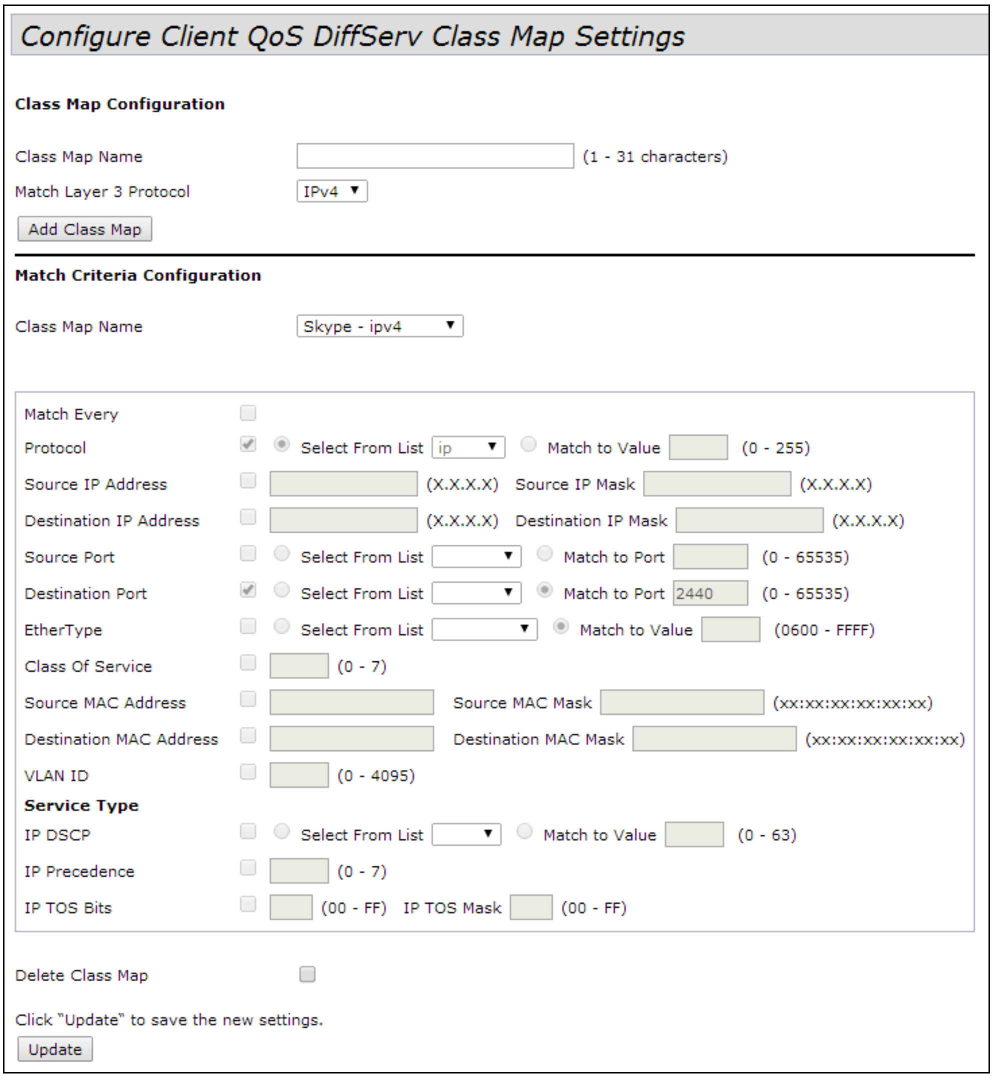
Field	***Description***
Client QoS Global Admin Mode	Enable or disable Client QoS operation on the AP. Changing this setting will not affect the WMM settings you configure on the QoS page.
Radio	Select Radio 1 or Radio 2 to specify which radio to configure.
VAP	Specify the VAP that will have the Client QoS settings that you configure. The QoS settings you configure for the selected VAP will not affect clients that access the network through other VAPs.
QoS Mode	Enable or disable QoS operation on the VAP selected in the VAP menu. QoS must be enabled globally (from the **Client QoS Global Admin Mode** *Field*) and on the VAP (**QoS Mode** *Field*) for the Client QoS settings to be applied to wireless clients.
Bandwidth Limit Down	Enter the maximum allowed transmission rate from the AP to the wireless client in bits per second. The valid range is 0-1331200 Kbps. A non-zero configured value is rounded down to the nearest 64 Kbps value for

	use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.
Bandwidth Limit Up	Enter the maximum allowed client transmission rate to the AP in bits per second. The valid range is 0-1331200 Kbps. A non-zero configured value is rounded down to the nearest 64 Kbps value for use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.
DiffServ Policy Down	Select the name of the DiffServ policy applied to traffic from the AP in the outbound(down) direction.
DiffServ Policy Up	Select the name of the DiffServ policy applied to traffic sent to the AP in the inbound (up) direction.

Click **Update** to save the new settings.

12.2 «Class Map» submenu

Use the **Class Map** page to add a new Diffserv class name, or to rename or delete an existing class, and define the criteria to associate with the DiffServ class.



Configure Client QoS DiffServ Class Map Settings

Class Map Configuration

Class Map Name (1 - 31 characters)

Match Layer 3 Protocol IPv4 ▼

Add Class Map

Match Criteria Configuration

Class Map Name Skype - ipv4 ▼

Match Every	□	
Protocol	☑	● Select From List ip ▼ ○ Match to Value (0 - 255)
Source IP Address	□	(X.X.X.X) Source IP Mask (X.X.X.X)
Destination IP Address	□	(X.X.X.X) Destination IP Mask (X.X.X.X)
Source Port	□	○ Select From List ▼ ○ Match to Port (0 - 65535)
Destination Port	☑	○ Select From List ▼ ● Match to Port 2440 (0 - 65535)
EtherType	□	○ Select From List ▼ ● Match to Value (0600 - FFFF)
Class Of Service	□	(0 - 7)
Source MAC Address	□	Source MAC Mask (xx:xx:xx:xx:xx:xx)
Destination MAC Address	□	Destination MAC Mask (xx:xx:xx:xx:xx:xx)
VLAN ID	□	(0 - 4095)
Service Type		
IP DSCP	□	○ Select From List ▼ ○ Match to Value (0 - 63)
IP Precedence	□	(0 - 7)
IP TOS Bits	□	(00 - FF) IP TOS Mask (00 - FF)

Delete Class Map □

Click "Update" to save the new settings.

Update

Field	*Description*
Class Map Configuration	
Class Map Name	Enter a Class Map Name to add. The name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon.
Match Layer 3 Protocol	Specify whether to classify IPv4 or IPv6 packets.
Match Criteria Configuration	
Class Map Name	Select name of the class to configure. Use the *Field*s in the **Match Criteria Configuration** area to match packets to a class. Select the check box for each *Field* to be used as a criterion for a class and enter data in the related *Field*. You can have multiple match criteria in a class. **Note:** The match criteria *Field*s that are available depend on whether the class map is an IPv4 or IPv6 class map.
Match Every	Select **Match Every** to specify that the match condition is true to all the parameters in an L3 packet. All L3 packets will match an **Match Every** match condition.
Protocol	Select the **Protocol** *Field* to use an L3 or L4 protocol match condition based on the value of the IP Protocol *Field* in IPv4 packets or the Next Header *Field* of IPv6 packets. Once you select the *Field*, choose the protocol to match by keyword or enter a protocol ID. **Select From List** Select one of the following protocols from the list: IP, ICMP, IPv6. ICMPv6, IGMP, TCP, UDP. **Match to Value** To match a protocol that is not listed by name, enter the protocol ID. The protocol ID is a standard value assigned by the IANA. The range is a number from 0-255.
IPv4 Class Maps	
Source IP Address	Select this *Field* to require a packet's source IP address to match the address listed here. Enter an IP address in the appropriate *Field* to apply this criteria.
Source IP Mask	Enter the source IP address mask. The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP Address to use for matching against packet content. A DiffServ mask of 255.255.255.255 indicates that all bits are important, and a mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example 192.168.10.0/24), use a mask of 255.255.255.0.
Destination IP Address	Select this *Field* to require a packet's destination IP address to match the address listed here. Enter an IP address in the appropriate *Field* to apply this criteria.
Destination IP Mask	Enter the destination IP address mask. The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP Address to use for matching against packet content. A DiffServ mask of 255.255.255.255 indicates that all bits are important, and a mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example 192.168.10.0/24), use a mask of 255.255.255.0.

IPv6 Class Maps	
Source IPv6 Address	Select this *Field* to require a packet's source IPv6 address to match the address listed here. Enter an IPv6 address in the appropriate *Field* to apply this criteria.
Source IPv6 Prefix Length	Enter the prefix length of the source IPv6 address.
Destination IPv6 Address	Select this *Field* to require a packet's destination IPv6 address to match the address listed here. Enter an IPv6 address in the appropriate *Field* to apply this criteria.
Destination IPv6 Prefix Length	Enter the prefix length of the destination IPv6 address.
IPv6 Flow Label	Flow label is 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify quality-of-service handling in routers (range 0 to 1048575).
IPv4 and IPv6 Class Maps	
Source Port	Select this *Field* to include a source port in the match condition for the rule. The source port is identified in the datagram header. Once you select the *Field*, choose the port name or enter the port number. **Select From List** Select the keyword associated with the source port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these keywords translates into its equivalent port number. **Match to Port** Enter the IANA port number to match to the source port identified in the datagramheader. The port range is 0-65535 and includes three different types of ports: 0-1023: Well Known Ports, 1024-49151: Registered Ports, 49152-65535: Dynamic and/or Private Ports
Destination Port	Select this *Field* to include a destination port in the match condition for the rule. Thedestination port is identified in the datagram header. Once you select the *Field*, choose the port name or enter the port number. **Select From List** Select the keyword associated with the destination port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these keywords translates into its equivalent port number. **Match to Port** Enter the IANA port number to match to the destination port identified in the datagram header. The port range is 0-65535 and includes three different types of ports: 0-1023: Well Known Ports, 1024-49151: Registered Ports, 49152-65535: Dynamic and/or Private Ports.
EtherType	Select the EtherType *Field* to compare the match criteria against the value in the header of an Ethernet frame. Select an EtherType keyword or enter an EtherType value to specify the match criteria. **Select from List Select** Select one of the following protocol types: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe. **Match to Value** Enter a custom protocol identifier to which packets are matched. The value is a four-digit hexidecimal number in the range of 0600-FFFF.
Class of Service	Select the *Field* and enter a class of service 802.1p user priority value to be matched for the packets. The valid range is 0-7.
Source MAC Address	Select this *Field* and enter the source MAC address to compare against an Ethernet frame.
Source MAC Mask	Enter the source MAC address mask specifying which bits in the destination

	MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.
Destination MAC Address	Select this *Field* and enter the destination MAC address to compare against an Ethernet frame.
Destination MAC Mask	Enter the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.
VLAN ID	Select the *Field* and enter a VLAN ID to be matched for packets. The VLAN ID range is 0-4095.
IPv4 Class Maps	
Service Type	You can specify one type of service to use in matching packets to class criteria.
IP DSCP	To use IP DSCP as a match criteria, select the check box and select a DSCP valuekeyword or enter a DSCP. **Select from List** Select from a list of DSCP types. **Match to Value** Enter a DSCP Value to match (0-63).
IP Precedence	Select this *Field* to match the packet's IP Precedence value to the class criteria IPPrecedence value. The IP Precedence range is 0-7.
IP TOS Bits	Select this *Field* and enter a value to use the packet's Type of Service bits in the IP header as match criteria. The TOS bit value ranges between (00-FF). The high-order three bits represent the IP precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.
IP TOS Mask	Enter an IP TOS mask value to perform a boolean AND with the TOS *Field* in the header of the packet and compared against the TOS entered for this rule. The TOS Mask can be used to compare specific bits (Precedence/Type of Service) from the TOS *Field* in the IP header of a packet against the TOS value entered for this rule. (00-FF).
Delete Class Map	Check to delete the class map selected in the **Class Map Name** menu. The class map cannot be deleted if it is already attached to a policy.

To delete a Class Map, select the **Delete Class Map** option and click **Update**.

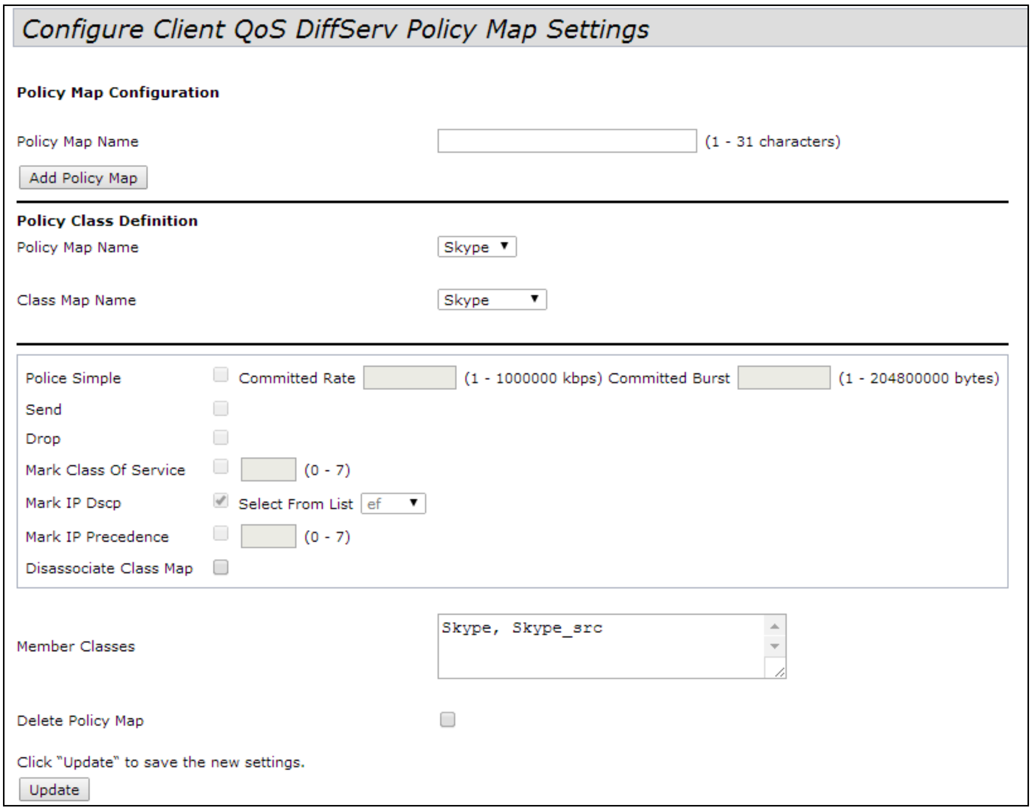
12.3 «Policy Map» submenu

Use the **Policy Map** page to create DiffServ policies and to associate a collection of classes with one or more policy statements.

The UAP supports up to 50 Policy Maps.

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class on the**Class Map** page. The processing is defined by a policy's attributes on the **Policy Map** page. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A Policy Map can contain up to 10 Class Maps. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.



Configure Client QoS DiffServ Policy Map Settings

Policy Map Configuration

Policy Map Name [ ] (1 - 31 characters)

Add Policy Map

Policy Class Definition

Policy Map Name: Skype ▼

Class Map Name: Skype ▼

Police Simple ☐ Committed Rate [ ] (1 - 1000000 kbps) Committed Burst [ ] (1 - 204800000 bytes)

Send ☐

Drop ☐

Mark Class Of Service ☐ [ ] (0 - 7)

Mark IP Dscp ☑ Select From List: ef ▼

Mark IP Precedence ☐ [ ] (0 - 7)

Disassociate Class Map ☐

Member Classes: Skype, Skype_src

Delete Policy Map ☐

Click "Update" to save the new settings.

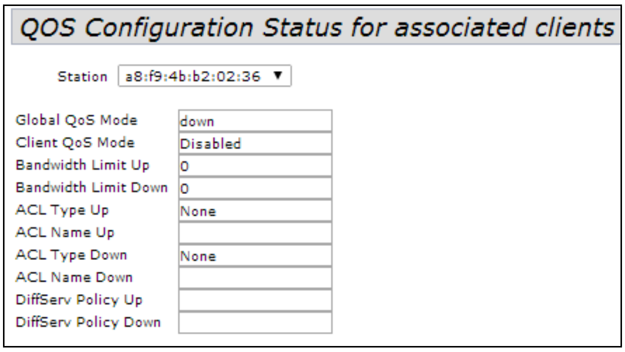
Update

Field	Description
Policy Map Name	Enter then name of the policy map to add. The policy map name can include from 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon.
Policy Map Name (Policy ClassDefinition)	Select the policy to associate with a member class.
Class Map Name (Policy ClassDefinition)	Select the member class to associate with this policy name.
Police Simple	Select this option to establish the traffic policing style for the class. The simple form of the policing style uses a single data rate and burst size, resulting in two outcomes: conform and nonconform. **Committed Rate** Enter the committed rate, in Kbps, to which traffic must conform. **Committed Burst** Enter the committed burst size, in bytes, to which traffic must conform.Ideally,burst size should be 1.5 times committed rate in bytes for Rate Limiting to work properly.For example,if committed rate is 1Gbps,then the committed burst size should be 187500000 bytes.
Send	Select **Send** to specify that all packets for the associated traffic stream are to be forwarded if the class map criteria is met.
Drop	Select **Drop** to specify that all packets for the associated traffic stream are to be dropped if the class map criteria is met.
Mark Class of Service	Select this *Field* to mark all packets for the associated traffic stream with the specified class of service value in the priority *Field* of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0-7.
Mark IP DSCP	Select this *Field* to mark all packets for the associated traffic stream with the IP DSCP value you select from the list or specify. **Select from List**

	Select from a list of DSCP types. **Match to Value** Enter a DSCP Value to match (0-63).
Mark IP Precedence	Select this *Field* to mark all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0-7.
Disassociate Class Map	Select this option and click **Update** to remove the class selected in the Class Map Name menu from the policy selected in the Policy Map Name menu.
Member Classes	Lists all DiffServ classes currently defined as members of the selected policy. If no class is associated with the policy, the *Field* is empty.
Delete Policy Map	Select this *Field* to delete the policy map showing in the Policy Map Name menu.

To delete a Policy Map, select the **Delete Policy Map** option and click **Update**.

12.4 «Client Configuration» submenu



QOS Configuration Status for associated clients

Station: a8:f9:4b:b2:02:36 ▼

Global QoS Mode: down
Client QoS Mode: Disabled
Bandwidth Limit Up: 0
Bandwidth Limit Down: 0
ACL Type Up: None
ACL Name Up:
ACL Type Down: None
ACL Name Down:
DiffServ Policy Up:
DiffServ Policy Down:

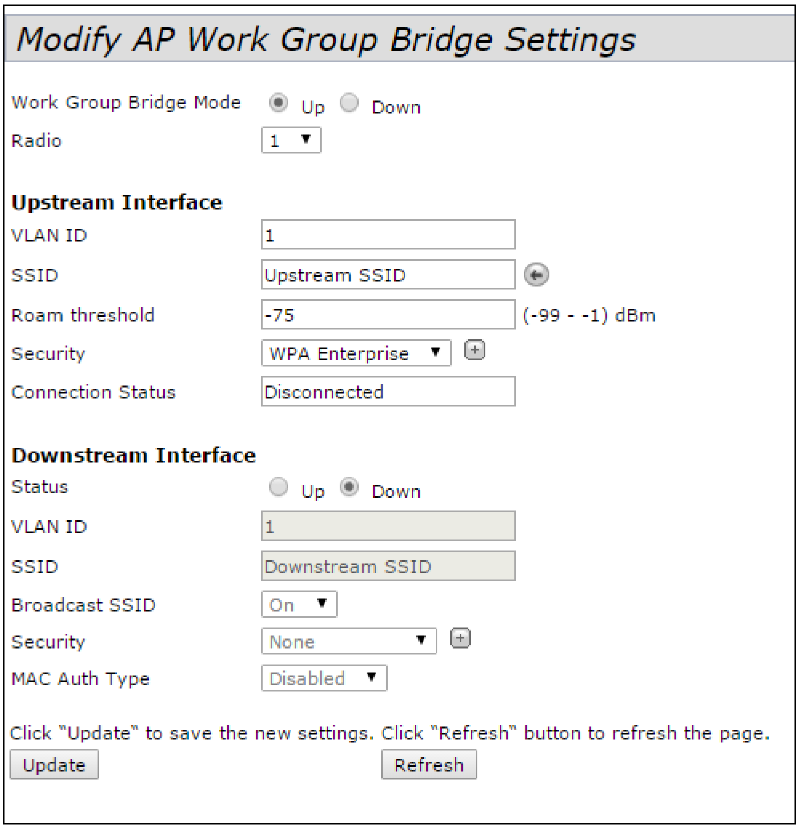
Field	*Description*
Station	The Station menu contains the MAC address of each client currently associated with the AP. To view the QoS settings applied to a client, select its MAC address from the list.
QoS Mode	Shows whether the QOS mode for the selected client is enabled or disabled. **Note:** For the Qos Mode to be enabled on a client, it must be globally enabled on the AP and enabled on the VAP the client is associated with. Use the **VAP QoS Parameters** page to enable the QoS Global Admin mode and the per-VAP QoS Mode.
Bandwidth Limit Up	Shows the maximum allowed transmission rate from the client to the AP in bits per second (bps). The valid range is 0-1331200 Kbps.
Bandwidth Limit Down	Shows the maximum allowed transmission rate from the AP to the client in bits per second (bps). The valid range is 0-1331200 Kbps.
ACL Type Up	Shows the type of ACL that is applied to traffic in the inbound (client-to-AP) direction, which can be one of the following: IPv4: The ACL examines IPv4 packets for matches to ACL rules. IPv6: The ACL examines IPv6 packets for matches to ACL rules. MAC: The ACL examines layer 2 frames for matches to ACL rules.
ACL Name Up	Shows the name of the ACL applied to traffic entering the AP in the inbound direction. When a packet or frame is received by the AP, the ACL's rules are checked for a match. The packet or frame is processed if it is permitted and discarded if it is denied.
ACL Type Down	Shows the type of ACL to apply to traffic in the outbound (AP-to-client) direction, which can be one of the following: IPv4: The ACL examines IPv4 packets for matches to ACL rules. IPv6: The ACL examines IPv6 packets for matches to ACL rules.

	MAC: The ACL examines layer 2 frames for matches to ACL rules.
ACL Name Down	Shows the name of the ACL applied to traffic in the outbound direction. After switching the packet or frame to the outbound interface, the ACL's rules are checked for a match. The packet or frame is transmitted if it is permitted and discarded if it is denied.
DiffServ Policy Up	Shows the name of the DiffServ policy applied to traffic sent to the AP in the inbound (client-to-AP) direction.
DiffServ Policy Down	Shows the name of the DiffServ policy applied to traffic from the AP in the outbound (AP-to-client) direction.

13 «WORK GROUP BRIDGE» MENU

13.1 «Work group bridge» submenu

Use the **Work Group Bridge** page to configure the Work Group Bridge mode on the AP and to configure the settings that allow the AP to serve as a bridge between remote clients and the wireless LAN.

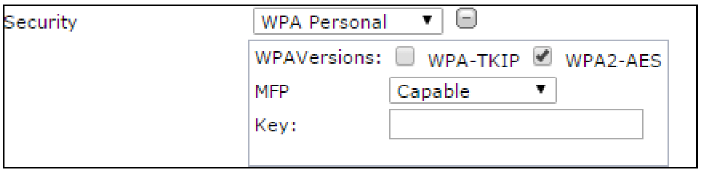


Modify AP Work Group Bridge Settings

Work Group Bridge Mode	● Up ○ Down
Radio	1 ▼
Upstream Interface	
VLAN ID	1
SSID	Upstream SSID
Roam threshold	-75 (-99 - -1) dBm
Security	WPA Enterprise ▼
Connection Status	Disconnected
Downstream Interface	
Status	○ Up ● Down
VLAN ID	1
SSID	Downstream SSID
Broadcast SSID	On ▼
Security	None ▼
MAC Auth Type	Disabled ▼

Click "Update" to save the new settings. Click "Refresh" button to refresh the page.

Field	*Description*
Work Group Bridge Mode	Set the administrative mode of the Work Group Bridge feature.
Radio	Select the radio on which to configure Work Group Bridge mode.
Upstream Interface	
VLAN ID	The VLAN associated with the BSS.
SSID	The SSID of the Basic Service Set (BSS). The BSS includes upstream access point and all of its connected clients (STAs).
Security	The type of security to use for authenticating as a client station on the upstream UAP. Choices are: • None; • Static WEP; • WPA Personal; • WPA Enterprise.
Connection Status	The Infrastructure Client Interface will be associated to the upstream UAP with theconfigured credentials. The UAP may obtain its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address. The Connection Status *Field* indicates whether the WAP is connected to the upstream UAP. Click **Refresh** to view the latest connection status.

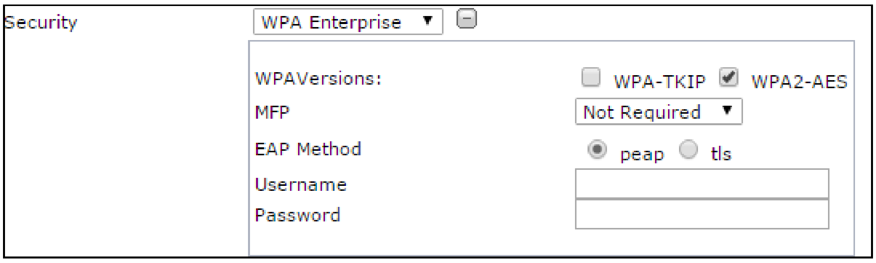


Security: WPA Personal

WPAVersions: □ WPA-TKIP ☑ WPA2-AES

MFP: Capable

Key:



Security: WPA Enterprise

WPAVersions: □ WPA-TKIP ☑ WPA2-AES

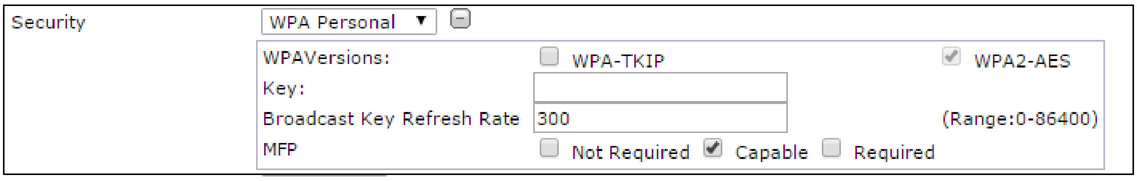
MFP: Not Required

EAP Method: ● peap ○ tls

Username:

Password:

Field	*Description*
Work Group Bridge Mode	Set the administrative mode of the Work Group Bridge feature.
Radio	Select the radio on which to configure Work Group Bridge mode.
Upstream Interface	
VLAN ID	The VLAN associated with the BSS.
SSID	The SSID of the Basic Service Set (BSS). The BSS includes upstream access point and all of its connected clients (STAs).
Security	The type of security to use for authenticating as a client station on the upstream UAP. Choices are: • None; • Static WEP; • WPA Personal; • WPA Enterprise.
Connection Status	The Infrastructure Client Interface will be associated to the upstream UAP with theconfigured credentials. The UAP may obtain its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address. The Connection Status *Field* indicates whether the WAP is connected to the upstream UAP. Click **Refresh** to view the latest connection status.
Downstream Interface	
Status	Enable (Up) or disable (Down) the administrative mode of the downstream interface. If the downstream interface is Down, wireless clients cannot connect to the UAP.
VLAN ID	The VLAN ID on the local AP interface. This VLAN ID should be the same VLAN ID asadvertised on the Infrastructure Client Interface.
SSID	Specify the SSID to broadcast to downstream clients.
Broadcast SSID	Select this option if you want the downstream SSID to be broadcast to wireless clients.
Security	The type of security downstream clients use to authenticate with the UAP. Choices are: • None; • WPA Personal; • WPA Enterprise.
MAC Auth Type	Select one of the following options for MAC authentication:

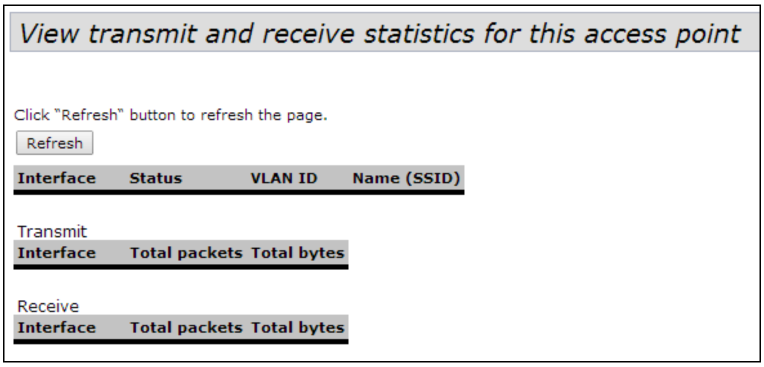


Security	WPA Personal ▼ ⊟		
WPAVersions:	□ WPA-TKIP		☑ WPA2-AES
Key:			
Broadcast Key Refresh Rate	300		(Range:0-86400)
MFP	□ Not Required	☑ Capable	□ Required

Click **Update** to save the new settings. Click **Refresh** button to refresh the page.

13.2 «Workgroup Bridge Transmit/Receive» submenu

The **Workgroup Bridge Transmit/Receive** page displays packet and byte counts for traffic between stations on a workgroup bridge.



View transmit and receive statistics for this access point

Click "Refresh" button to refresh the page.

Interface	Status	VLAN ID	Name (SSID)

Transmit

Interface	Total packets	Total bytes

Receive

Interface	Total packets	Total bytes

The information in the following table is available for each network interface that is configured as a workgroup bridge interface.

Field	*Description*
Interface	Name of the Ethernet or VAP interface.
Status	Whether the interface is disconnected or is administratively configured as up or down.
VLAN ID	Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same UAP. The VLAN ID is set on the VAP tab. See Configuring VAPs.
Name (SSID)	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP tab. See Configuring VAPs.
Transmit and Receive Statistics	
Total Packets	The total number of packets bridged between the wired clients in the workgroup bridge and the wireless network.
Total Bytes	The total number of bytes bridged between the wired clients in the workgroup bridge and the wireless network.

Click **Refresh** to update the screen and display the most current information.

TECHNICAL SUPPORT SERVICE

For technical assistance in issues related to handling of EltexAlatau Ltd. equipment please address to Service Centre of the company:

9 Ibragimova street, Almaty, Republic of Kazakhstan, 050032,
Phone:
+7(727) 320-18-40
+7(727) 320-18-38
E-mail: info@eltexalatau.kz

In official website of the EltexAlatau Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center:

http://www.eltexalatau.kz/en