Wireless access point

WEP-2ac, WEP-2ac Smart

Quick guide

Firmware version 1.23.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 Annotation

This manual contains the following information:

- connection to WEP-2ac web interface;
- configuration of WEP-2ac network parameters;
- WEP-2ac firmware update;
- SNMP configuration;
- wireless interfaces configuration (operation mode, band);
- virtual access points configuration;
- monitoring of wireless network main parameters.

The manual provides an example of access point configuration without using a softWLC controller. The following scheme is given as an example.

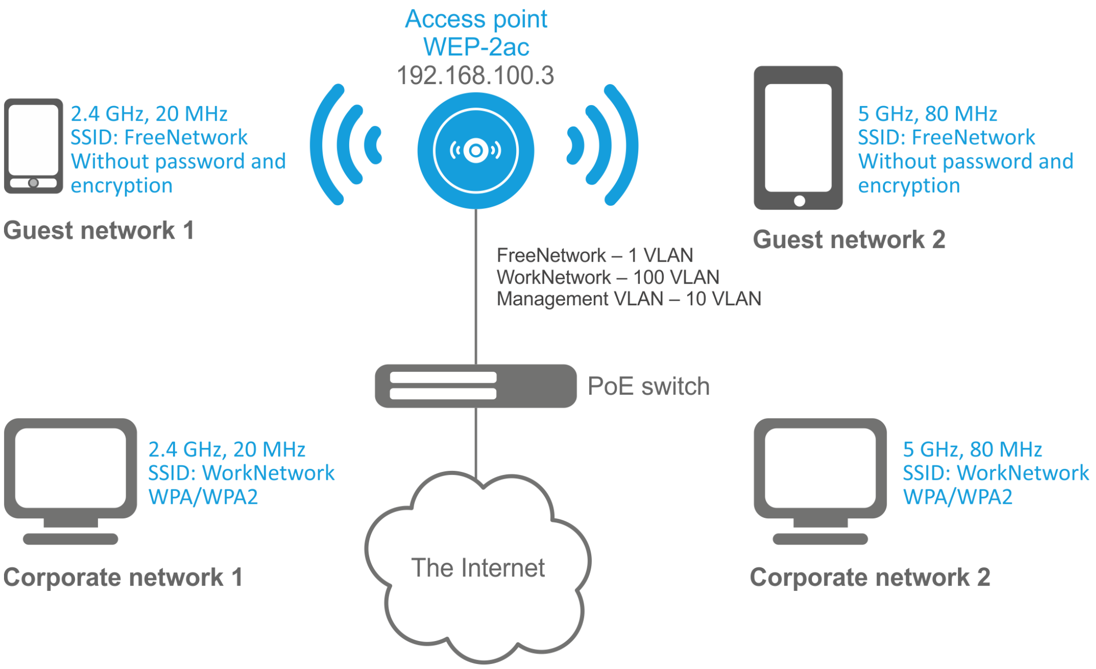


Figure 1 – Example of network configuration

Type of the network	VLAN used	SSID used	Encryption/ authorization by password
Inner corporate wireless network using 2.4 and 5 GHz bands. The network is isolated from other guest networks. To connect to the network, password authorization is required. The network is dedicated to secure data exchange among company staff.	100	WorkNetwork	WPA/WPA2
Guest wireless network using 2.4 and 5 GHz bands. The network does not require password authorization. It is dedicated to connect users with standard wireless gadgets to a public network for Internet access, for instance.	1 (without VLAN)	FreeNetwork	No encryption and authorization

To perform the configuration, a PC with access to the device via Ethernet and any web browser (Internet Explorer, Firefox, Google Chrome, Opera, etc.) are required.

2 Installation order

This section defines safety rules, installation recommendations, setup procedure and the device starting procedure.

2.1 Safety rules

1. Do not install the device close to heat sources or in rooms with temperature below 5 °C or above 40 °C.
2. Do not use the device in places with high humidity. Do not expose the device to smoke, dust, water, mechanical vibrations or shocks.
3. Do not open the device case. There are no user serviceable parts inside.

> ❗ Do not cover ventilation holes and do not put other objects on the device in order to prevent overheating of device components.

2.2 Installation recommendations

1. The recommended mounting position: horizontal, on a ceiling.
2. Before installing and enabling the device, check it for visible mechanical defects. If defects are observed, stop the device installation, draw up corresponding act and contact the supplier.
3. If the device has been exposed for a long time at a low temperature, it must be left to stand for two hours at room temperature before use. After a long stay of the device in conditions of high humidity, let it stand under normal conditions for at least 12 hours before switching on.
4. During the device installation, follow these rules to ensure the best Wi-Fi coverage:
    a. Install the device at the center of a wireless network;
    b. Minimize the number of obstacles (walls, roof, furniture and etc.) between access point and other wireless network devices;
    c. Do not install the device near (about 2 m) electrical and radio devices;
    d. It is not recommended to use radiophone and other equipment operating on the frequency of 2.4 GHz, 5 GHz in Wi-Fi effective radius;
    e. Obstacles like glass/metal constructions, brick/concrete walls, water cans and mirrors can significantly reduce Wi-Fi action radius. It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.
5. During the installation of several access points, cell action radius must overlap with action radius of a neighboring cell at level of -65 ÷ -70 dBm. Decreasing of the signal level on cells borders to -75 dBm is permitted if it involves the use of VoIP, streaming video and other traffic that is sensitive to losses in wireless network.

2.3 Device installation

The device should be attached to plain surface (wall or ceiling) in accordance with the safety instruction and recommendations listed above.
The device delivery package includes required mounting kit to attach the device to plain surface.

2.3.1 Wall mounting

1. Fix the bracket (included in the delivery package) to the wall:

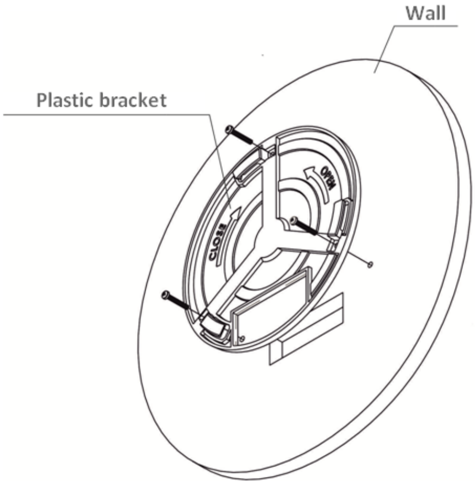


Figure 7 – Attaching the bracket to a wall

   a. The figure shows the bracket allocation;
   b. When installing the bracket, pass wires through the corresponding grooves of the bracket, see figure 7;
   c. Pass the wires into the corresponding grooves on the bracket while installing the bracket. Screw the brackets to the device surface by using screwdriver.

2. Install the device.

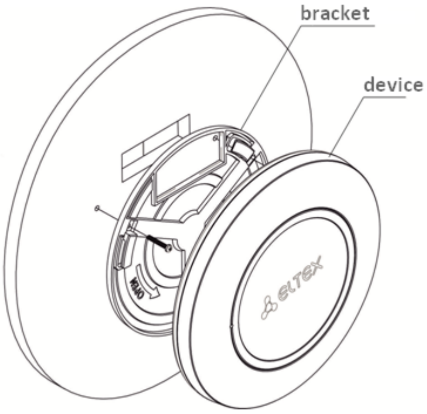
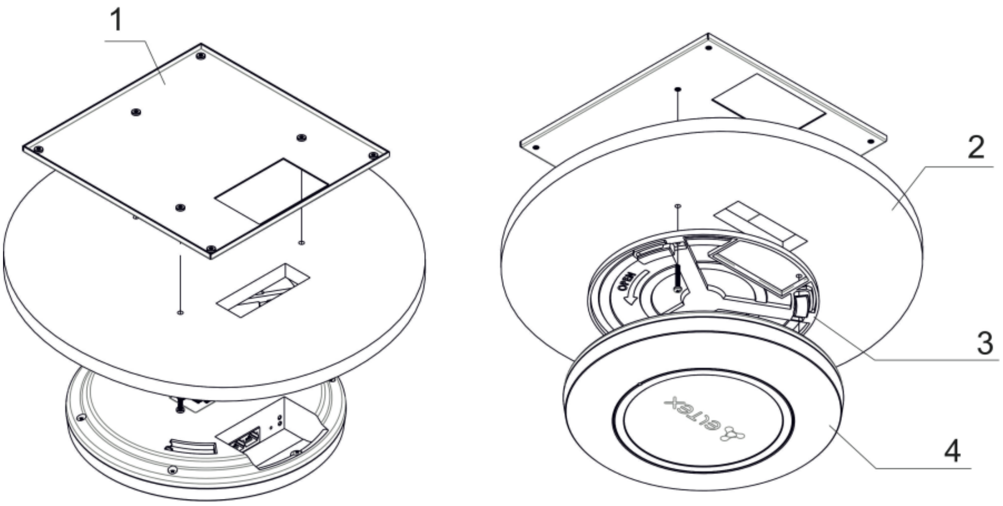


Figure 8 – Device installation (front view)

1. Connect cables to corresponding connector of the device.
   Description of the connectors is given in Design section of the User manual.
2. Align the device and bracket together, fix the position, turning clockwise.

2.3.2 Installing to false ceiling

❗ It is not recommended to place the device inside a false ceiling as metal frame causes multipath signal propagation and signal attenuation.



1 – metal bracket; 2 – Armstrong panel; 3 – plastic bracket; 4 – device.

Figure 9 – Mounting to a false ceiling

1. Fasten metal and plastic bracket on a ceiling as shown in the figure 9.
   a. The plastic bracket (**3**) should be joined with the metal one (**1**) on the ceiling in the following order: metal bracket -> Armstrong panel -> plastic bracket.
   b. Cut the hole in the Armstrong panel. The size of the hole should be equal to hole of metal bracket. Conduct wires through the hole.
   c. Align holes in metal bracket with holes of Armstrong panel and plastic bracket. Align together three screw holes on the plastic bracket and the screw holes on the metal bracket. Screw the brackets to the device surface by using a screwdriver.
2. Install the device.
   a. Connect cables to corresponding connector of the device. Description of the connectors is given in Design section of the User manual.
   b. Align the device and plastic bracket together, fix the position, turning clockwise.

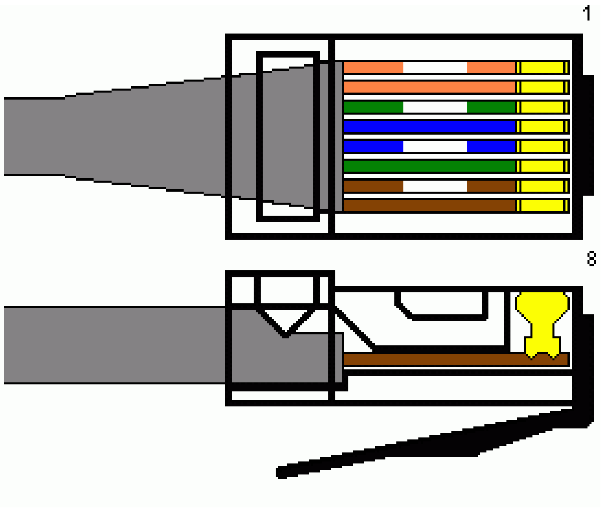
2.3.3 Removing the device from the bracket

For removing the device from the bracket:

1. Turn the device counterclockwise;
2. Remove the device.

2.3.4 **RJ-45 pinout**

The next scheme is used for twisted-pair wiring.

RJ-45 connector	
	Side A: 1. white orange; 2. orange; 3. white green; 4. blue; 5. white blue; 6. green; 7. white brown; 8. brown.

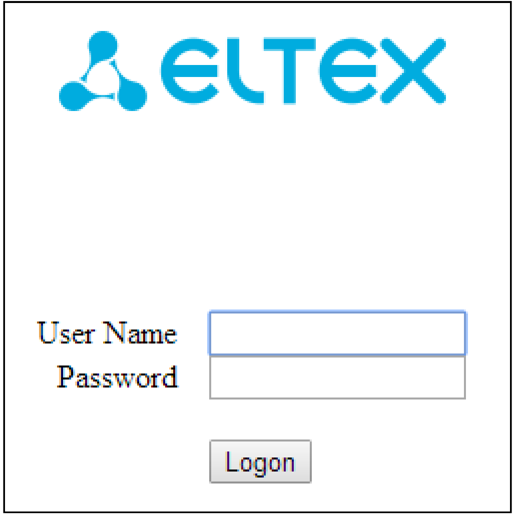
3 Connecting to the web interface

Connect network cable to the PoE interface of the access point and to the PoE switch/injector. Next, connect a PC to the injector or switch.

1. Open a web browser, for example, Firefox, Opera, Chrome.
2. Enter the device IP address in the browser address bar.

   > ✓ IP address by default: 192.168.1.10, subnet mask: 255.255.255.0.
   > The device can obtain IP address via DHCP. Until then, it is available at the factory IP address.

   If the connection has been performed successfully, the authorization page will be displayed:



3. Enter username to 'User Name' field and password to 'Password' field.

   > ✓ Factory default authorization settings: User Name – *admin*, Password – *password.*

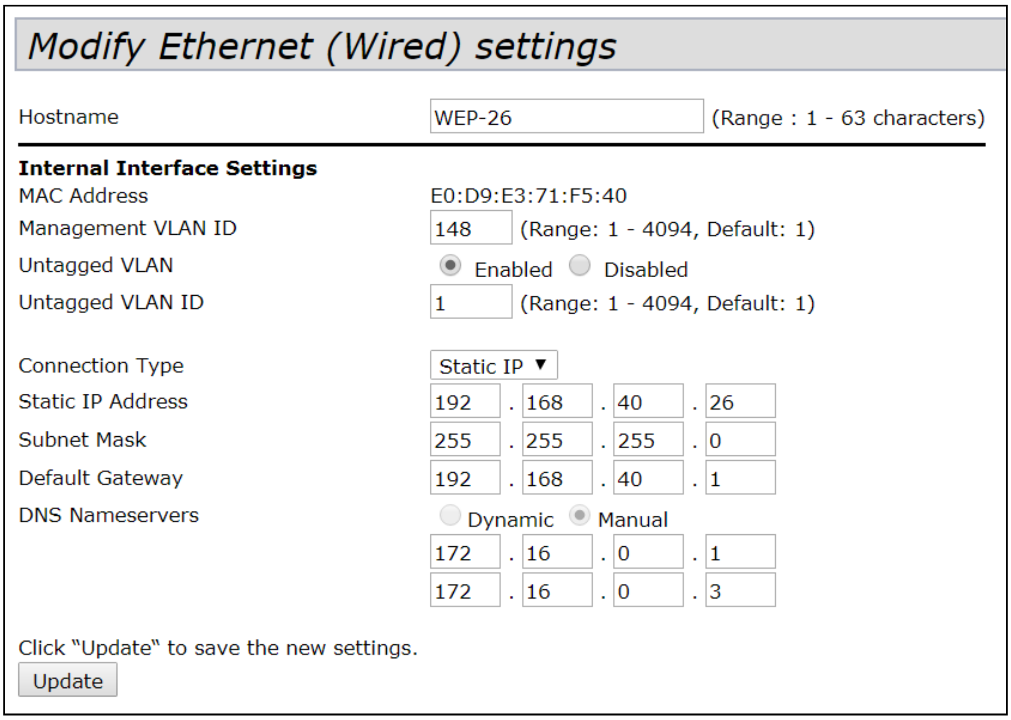
4. Click the Logon button.

A menu for monitoring the status of the device will open in a browser window.

> ❗ If after entering the IP address in the browser bar, the authorization page does not appear, check the IP address on the PC/switch settings.
> If the device factory configuration was changed, reset the current settings. To do this, press and hold the 'F' button on the side panel of the device for 20 seconds. The color of the indicator should change to red – this means that the load is in progress.

4 Configuring network parameters

For remote management of WEP-2ac and WEP-2ac Smart, set network parameters of the device according to the settings of the network that you intend to use.
In the **Manage** menu, open **Ethernet Settings** tab and perform the following:



Modify Ethernet (Wired) settings

Hostname	WEP-26 (Range : 1 - 63 characters)
Internal Interface Settings	
MAC Address	E0:D9:E3:71:F5:40
Management VLAN ID	148 (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 . 40 . 26
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 40 . 1
DNS Nameservers	○ Dynamic ● Manual
	172 . 16 . 0 . 1
	172 . 16 . 0 . 3

Click "Update" to save the new settings.

- *Management VLAN ID* – specify VLAN number that will be used for access point management. In the given example VLAN 148 is used;
- *Connection Type* – select **Static IP** to set IP addresses for access points manually. If it is necessary to distribute IP addresses and other network parameters to access points via the DHCP protocol, set the **Connection Type** field to 'DHCP' and this will complete the configuration of the network part;
- *Static IP Address* – specify the IP address of WEP-2ac. In the given example, VLAN 10 address is **192.168.40.26**;
- *Subnet Mask* – specify the subnet mask. In the given example, subnet mask is **255.255.255.0**;
- *Default Gateway* – enter the IP address of the default gateway field. 192.168.40.1. In the given example, IP address of the default gateway is **192.168.40.1**.

To apply a new configuration and save setting to non-volatile memory, click **Update**.

After the configuration, WEP-2ac will be available in 10 VLAN via 192.168.40.26 address.

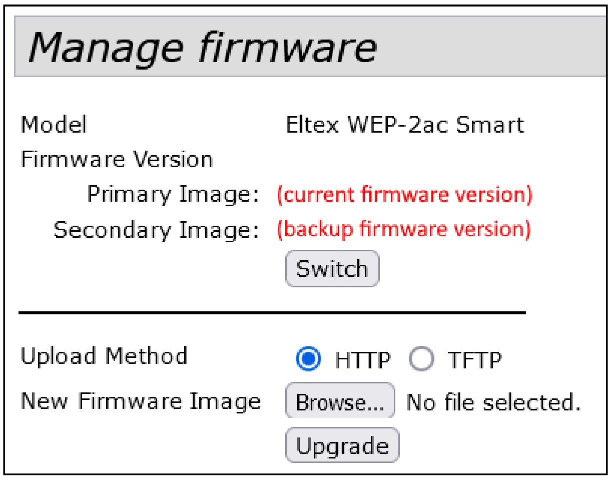
Before changing the settings, make sure that the managing computer has the access to the access point. If you make a mistake while changing the settings, undo them by resetting the access point to factory settings. To do this, press and hold 'F' button on the side panel of the device for 20 seconds until the indicator on the front panel is blinking.

5 Firmware upgrade

For correct operation of WEP-2ac and WEP-2ac Smart, it is recommended to update the firmware to the latest version.

✓ The relevance of the version installed on the device can be clarified on the official website of the manufacturer in the Download Center section or by contacting the manufacturer directly. Contact details are given on the last page of this manual.

After obtaining the relevant firmware version, in the **Maintenance** menu, open **Upgrade** tab and perform the following:



Manage firmware

Model: Eltex WEP-2ac Smart

Firmware Version

Primary Image: (current firmware version)

Secondary Image: (backup firmware version)

Upload Method: ● HTTP ○ TFTP

New Firmware Image: No file selected.

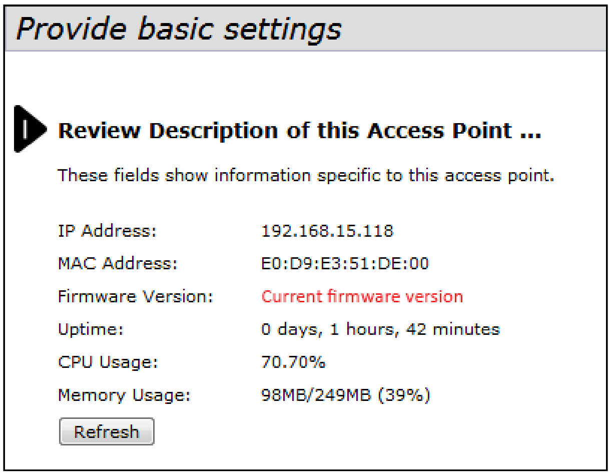
- *Upload Method* – check **HTTP**;
- *New Firmware Image* – click **Browse** button and select relevant firmware version in the window that opens.

To start the upgrade process, click **Upgrade**.

The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the upgrade is completed.

Do not switch off or reboot the device during the firmware update.

The current firmware version can be viewed in the **Basic Settings** menu. The current firmware version is indicated in the **Firmware Version** field.



Provide basic settings

Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 192.168.15.118

MAC Address: E0:D9:E3:51:DE:00

Firmware Version: Current firmware version

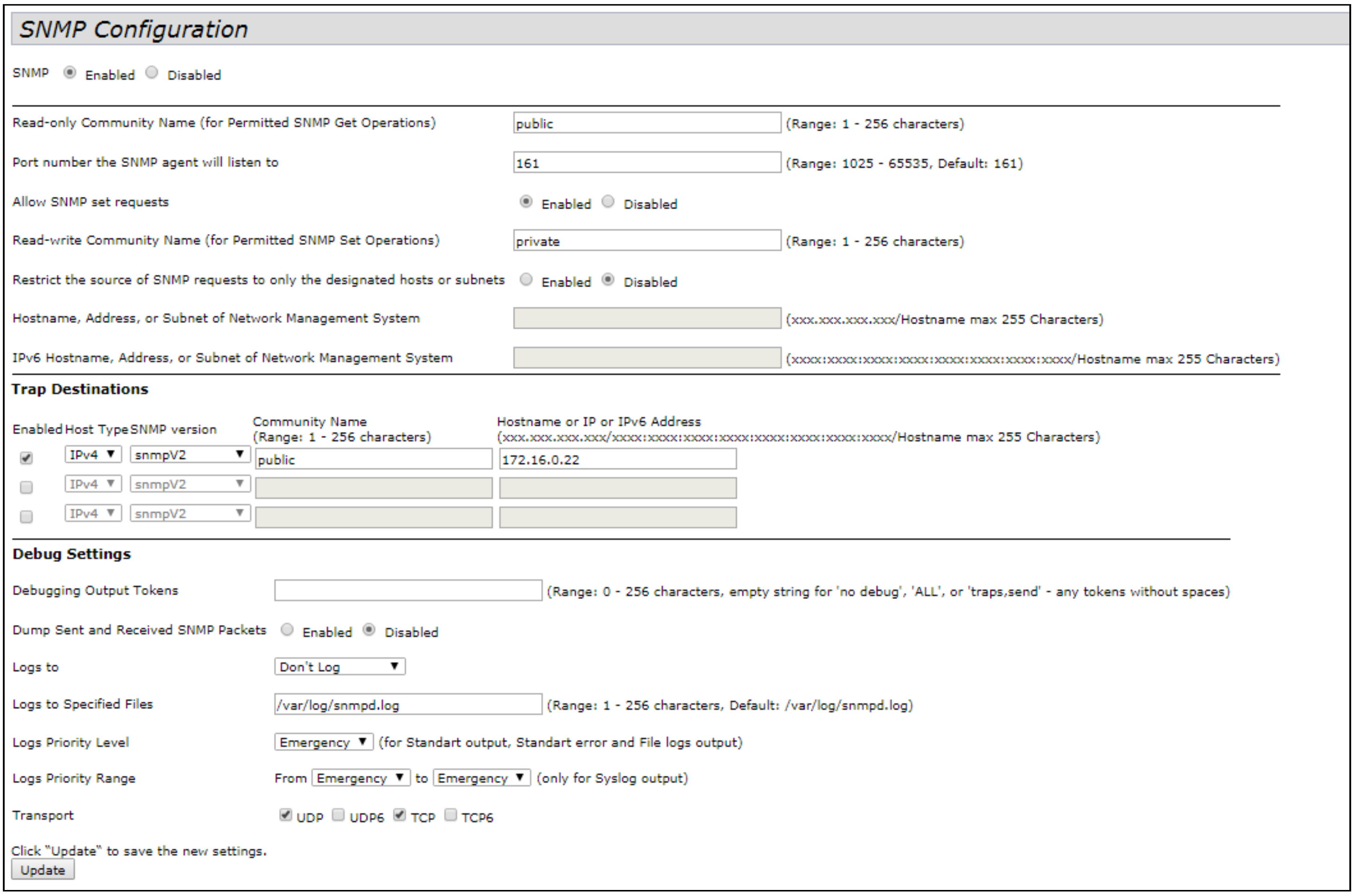
Uptime: 0 days, 1 hours, 42 minutes

CPU Usage: 70.70%

Memory Usage: 98MB/249MB (39%)

6 Configuring the SNMP service

SNMP service configuration is performed in the **SNMP** section of the **Services** menu.



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 ▼	public	172.16.0.22
□	IPv4 ▼	snmpV2 ▼		
□	IPv4 ▼	snmpV2 ▼		

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.

- *Restrict the source of SNMP requests to only the designated hosts or subnets* – reception of SNMP requests only from devices with specific IP address. Check **Enabled**;
- *Hostname, address, or subnet of Network Management System* – specify IP address of SNMP server from which SNMP commands will be transmitted.

In the **Trap Destinations** section, perform the following settings:

- Set the flag in the column with the **Enabled** heading;
- *Host Type* – specify whether the enabled host is an IPv4 host or an IPv6 host. In this example, IPv4 is selected;
- *SNMP version* – select the version of the SNMP protocol. In this example, the **snmpV2** protocol is selected;
- *Community name for traps* – set community name **public**;
- *Host name or IP or IPv6 Address* – check one of the fields for specifying traps receiver address and enter an IP address of the device to which WEP-2ac will send traps. In the given example, IP address to receive SNMP traps is **172.16.0.22**.

To apply a new configuration and save setting to non-volatile memory, click **Update**.

7 Configuring wireless interfaces

WEP-2ac and WEP-2ac Smart have 2 radio interfaces (Radio1 and Radio 2) that are capable to operate simultaneously. Radio 1 operates at 5 GHz band, Radio 2 – at 2.4 GHz.
The example of configuration of a network with the following characteristics is given below:

Radio1:

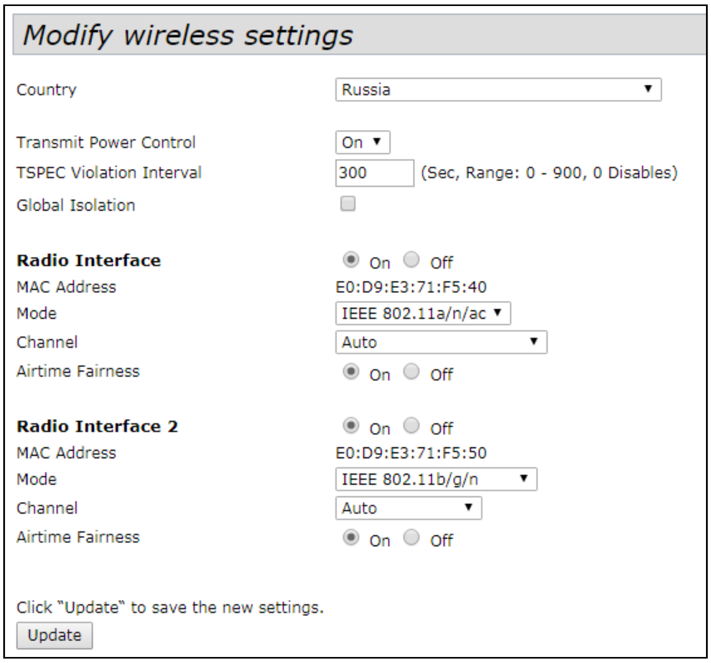
- Frequency range: 5 GHz;
- Standards: 802.11a/n/ac;
- Bandwidth: 80 MHz.

Radio2:

- Frequency range: 2.4 GHz;
- Standards: 802.11b/g/n;
- Bandwidth: 20 MHz.

To apply a new configuration and save setting to non-volatile memory, click **Update**.

In the **Manage** menu, open **Wireless Settings** tab and perform the following:



Modify wireless settings

Country: Russia

Transmit Power Control: On
TSPEC Violation Interval: 300 (Sec, Range: 0 - 900, 0 Disables)
Global Isolation: □

Radio Interface: ● On ○ Off
MAC Address: E0:D9:E3:71:F5:40
Mode: IEEE 802.11a/n/ac
Channel: Auto
Airtime Fairness: ● On ○ Off

Radio Interface 2: ● On ○ Off
MAC Address: E0:D9:E3:71:F5:50
Mode: IEEE 802.11b/g/n
Channel: Auto
Airtime Fairness: ● On ○ Off

Click "Update" to save the new settings.

- *Country* – name of the country where access point operates. Depending on the value set, the frequency band and transmitter power restrictions applicable in that country will be applied. The list of available frequency channels depends on the set country, which affects the automatic channel selection in the Channel = Auto mode. If the client equipment is licensed for use in another region, it will not be possible to establish a connection with the access point;
- *Transmit Power Control* – configuring the *Transmit Power Limit* parameter restrictions. Select **On** in the list.

Configuring Radio 1:

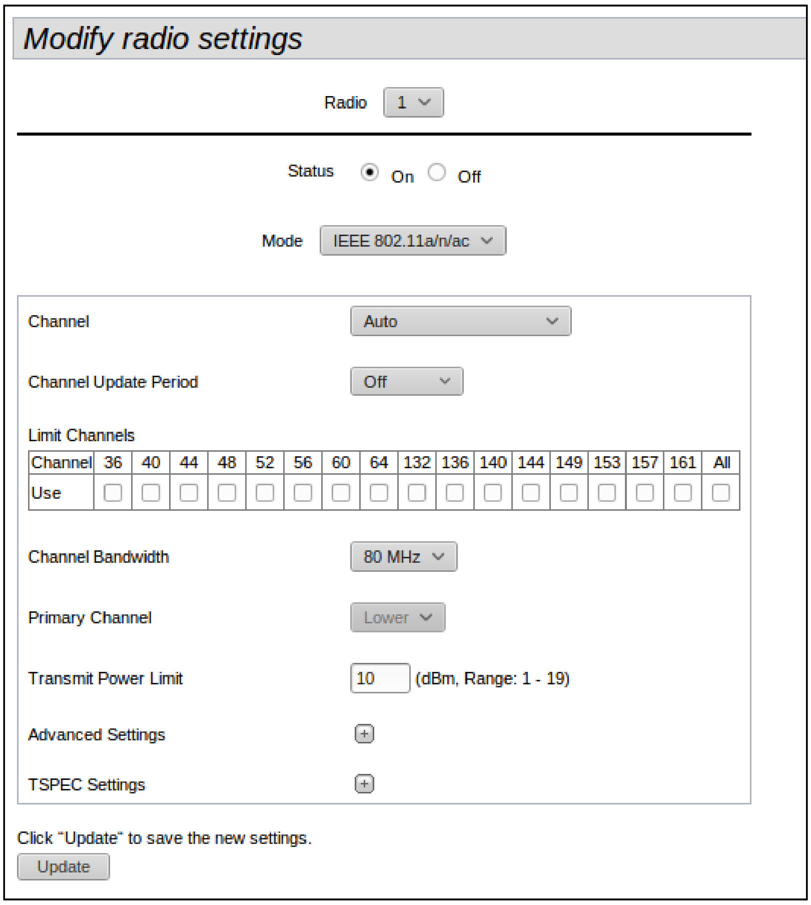
- *Radio Interface* – check the **On** box;
- *Mode* – select value **IEEE 802.11 a/n/ac**.

Configuring Radio 2:

- *Radio Interface 2* – check the **On** box;
- *Mode* – select value **IEEE 802.11 b/g/n**.

To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

In the **Manage** menu, open the **Radio** tab and perform the following:



Modify radio settings

Radio: 1

Status: ● On ○ Off

Mode: IEEE 802.11a/n/ac

Channel: Auto

Channel Update Period: Off

Limit Channels

Channel	36	40	44	48	52	56	60	64	132	136	140	144	149	153	157	161	All
Use	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Channel Bandwidth: 80 MHz

Primary Channel: Lower

Transmit Power Limit: 10 (dBm, Range: 1 - 19)

Advanced Settings ⊞

TSPEC Settings ⊞

Click "Update" to save the new settings.

Configuring Radio 1:

- *Radio* – select value **1**;
- *Channel Bandwidth* – set value **80 MHz**;

To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

Configuring Radio 2:

- *Radio* – select value **2**;
- *Channel Bandwidth* – set value **20 MHz.**

To apply a new configuration and save setting to non-volatile memory, click **Update**.

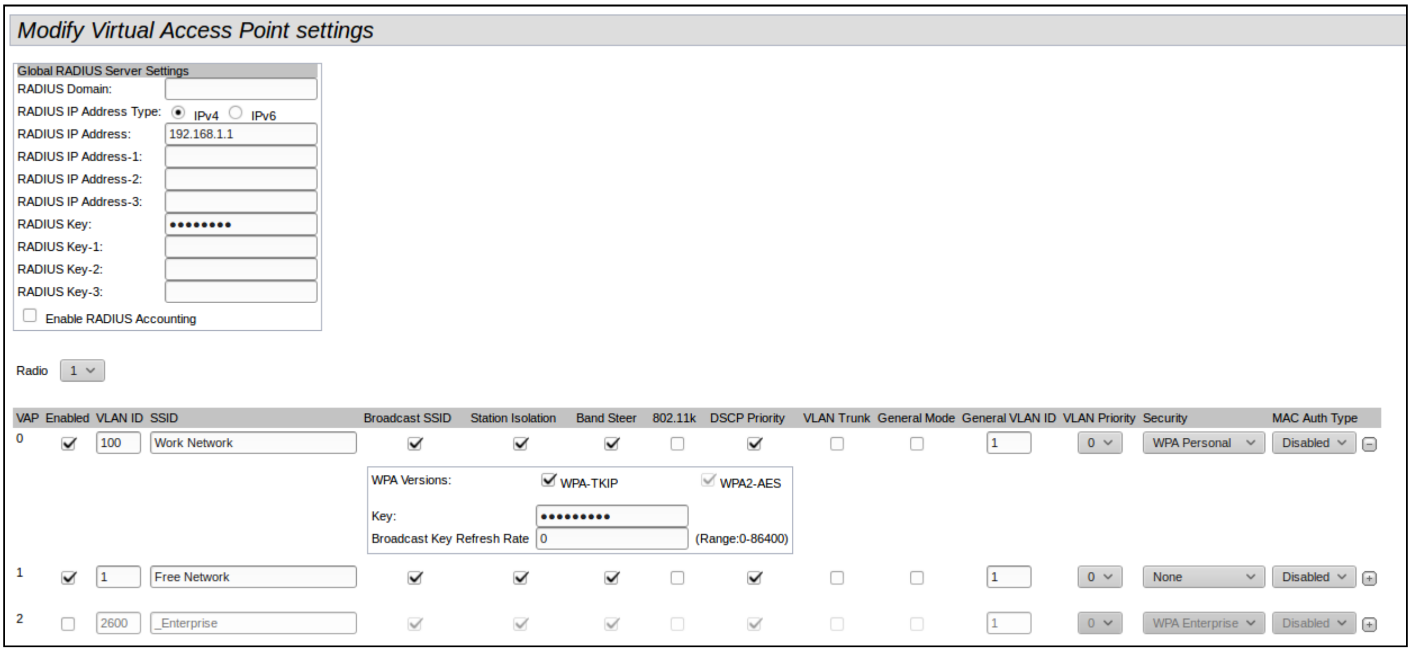
8 Configuring virtual access points

On each wireless interface, up to 16 virtual access points can be configured. Each access point may have individual name of wireless network (SSID) and type of authentication/authorization. According to the network diagram given in the figure 1, it is necessary to configure two virtual access points on Radio 1 and Radio 2.

Band Steer feature allows clients to have opportunity of operation at 2.4 GHz and 5 GHz to set priority of connection to 5 GHz band.

The following is necessary for Band Steer feature operation:
– configure radio interfaces for operation at different frequency ranges;
– create virtual access points (VAP) on each frequency range with the same SSID;
– when using encryption, make sure the passwords of the VAPs are the same;
– activate Band Steer feature on the access points.

In the **Manage** menu, open the **VAP** tab and perform the following:



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	Station Isolation	Band Steer	802.11k	DSCP Priority	VLAN Trunk	General Mode	General VLAN ID	VLAN Priority	Security	MAC Auth Type
0	☑	100	Work Network	☑	☑	☑	□	☑	□	□	1	0	WPA Personal	Disabled
1	☑	1	Free Network	☑	☑	☑	□	☑	□	□	1	0	None	Disabled
2	□	2600	_Enterprise	☑	☑	☑	□	☑	□	□	1	0	WPA Enterprise	Disabled

WPA Versions: ☑ WPA-TKIP ☑ WPA2-AES

Key: •••••••••

Broadcast Key Refresh Rate 0 (Range:0-86400)

Configuring Radio 1:

- *Radio* – select the radio interface on which VAP will be configured. Select **1.**
- *Enabled* – enable VAP. Check the boxes for VAP 0 and VAP1.
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled):
  - set VLAN ID value **100** for VAP 0;
  - set VLAN ID value **1** for VAP 1.
- *SSID* – wireless network name:
  - set SSID value **Work Network** for VAP 0;
  - set SSID value **Free Network** for VAP 1.
- *Station Isolation* – forbid packet transmission among access point clients. Check the box.
- *Band Steer* – set a priority of users connection to SSID configured at 5 GHz. Check the box.
- *Security* – secure network mode:
  - set **WPA Personal** value for VAP 0:
    - *Key* – set a password for this network connection. The password should be from 8 to 63 characters long.
  - set **None** value for VAP 1 – client device will be able to connect to this wireless network without password.

To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

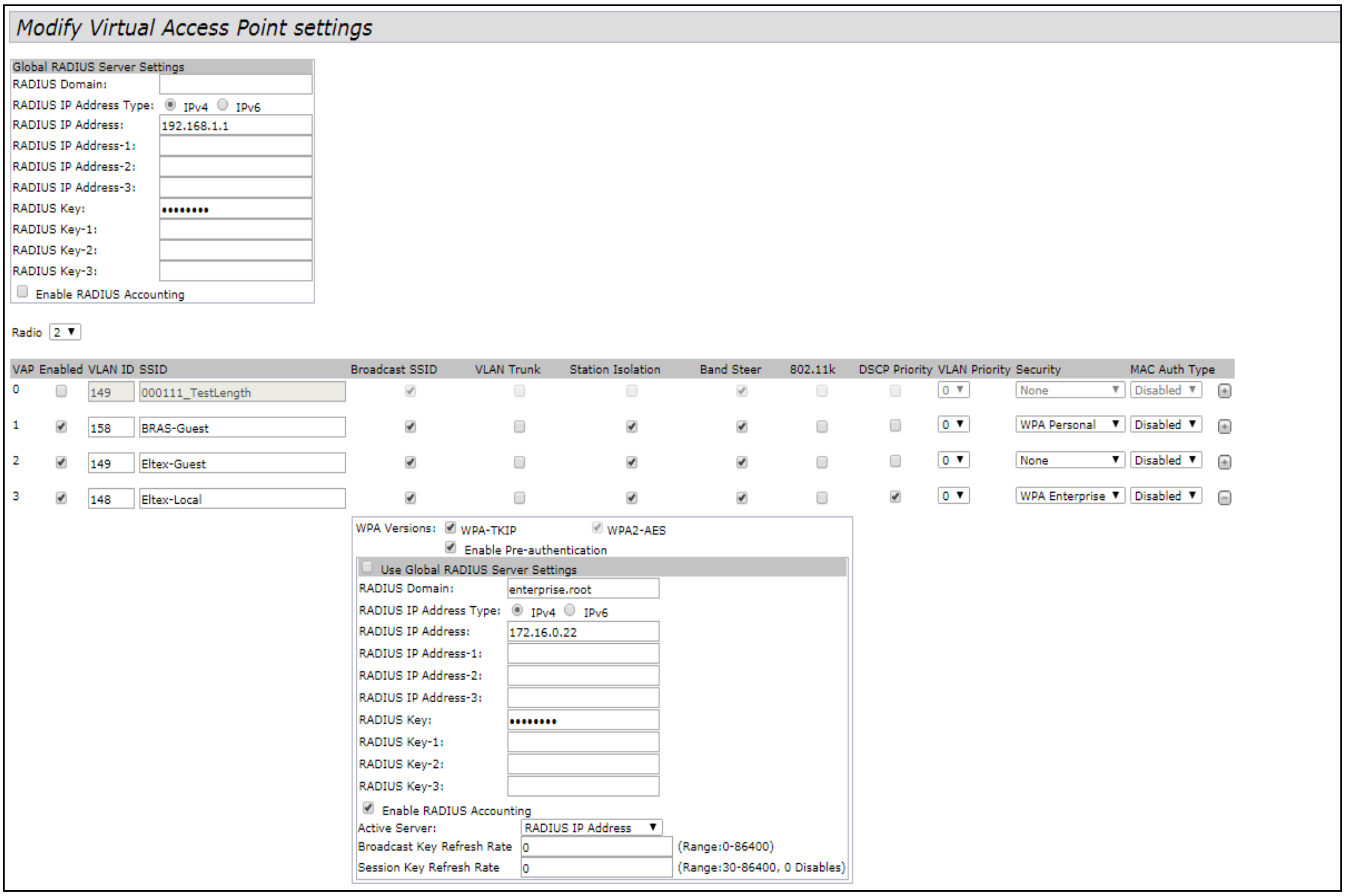
Configuration of Radio 2 is performed the same way. Select **2** value in **Radio** and perform the configuration as for the Radio 1 (given above). The password for 'Work Network' SSID should be the same for both VAP Radio 1 and VAP Radio 2.

After configuring VAP on Radio 2, click **Update**.

When using **WPA Enterprise** mode, the authorization is implemented through RADIUS server. The request on user connection to SSID with **WPA Enterprise** security mode is sent to a RADIUS server.
To connect to the RADIUS server, specify the following parameters in the *Global RADIUS server settings* table:

- *RADIUS Domain* – user domain;
- *RADIUS IP Address* – IP address of the RADIUS server;
- *RADIUS Key* – password to access the RADIUS server;
- *Enable RADIUS Accounting* – when checked, the Accounting messages will be sent to RADIUS server.

In the VAP settings, in the Security field, select **WPA Enterprise**, then check the box next to **Use Global RADIUS Server Settings** in the window that opens (if the window does not appear, click the '+' sign on the left in the VAP settings line).
If it is necessary to use a different RADIUS server for each VAP, then uncheck the box next to the **Use Global RADIUS Server Settings** and set the parameters for the RADIUS server listed above in the VAP settings window.



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 2 ▼

VAP	Enabled	VLAN ID	SSID	Broadcast SSID	VLAN Trunk	Station Isolation	Band Steer	802.11k	DSCP Priority	VLAN Priority	Security	MAC Auth Type	
0	□	149	000111_TestLength	☑	□	□	☑	□	□	0 ▼	None ▼	Disabled ▼	⊕
1	☑	158	BRAS-Guest	☑	□	☑	☑	□	□	0 ▼	WPA Personal ▼	Disabled ▼	⊕
2	☑	149	Eltex-Guest	☑	□	☑	☑	□	□	0 ▼	None ▼	Disabled ▼	⊕
3	☑	148	Eltex-Local	☑	□	☑	☑	□	☑	0 ▼	WPA Enterprise ▼	Disabled ▼	⊖

WPA Versions: ☑ WPA-TKIP ☑ WPA2-AES
☑ Enable Pre-authentication

□ Use Global RADIUS Server Settings

RADIUS Domain:	enterprise.root
RADIUS IP Address Type:	● IPv4 ○ IPv6
RADIUS IP Address:	172.16.0.22
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

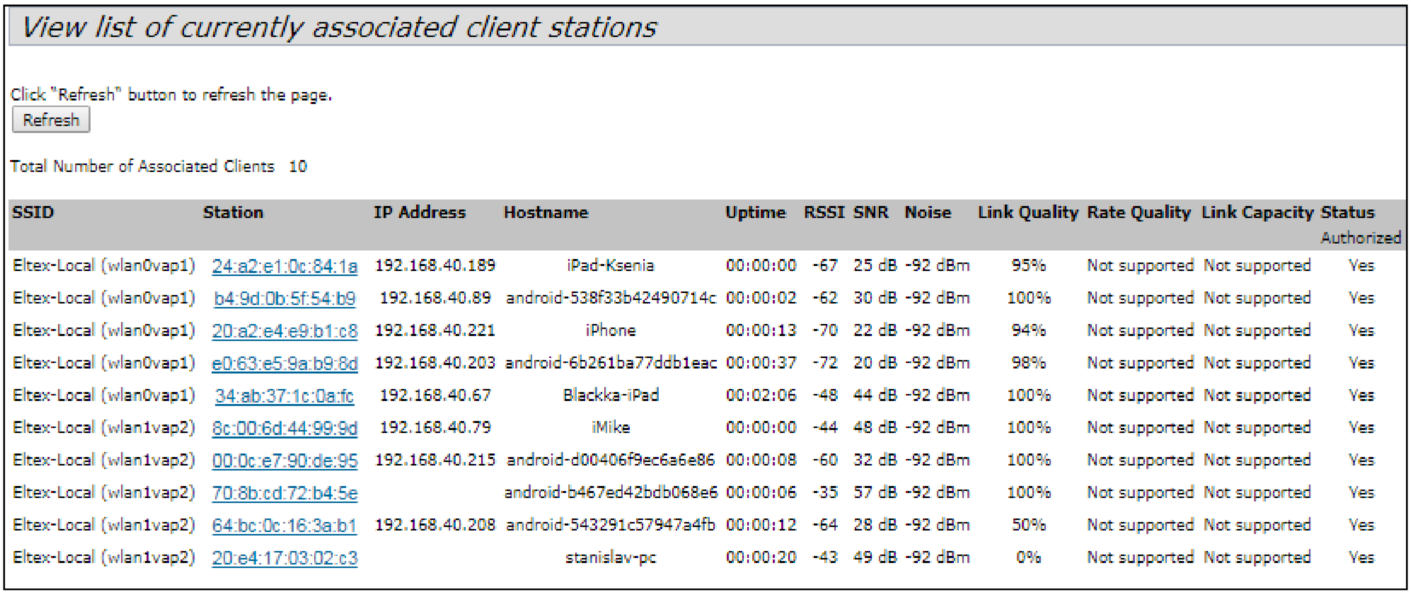
Active Server:	RADIUS IP Address ▼	
Broadcast Key Refresh Rate	0	(Range:0-86400)
Session Key Refresh Rate	0	(Range:30-86400, 0 Disables)

9 Monitoring of the general wireless network parameters

All clients connected to this access point can be viewed in the **Status** menu of the **Client Associations** tab.

Clicking on the client's MAC address reveals detailed information about the client's operation and statistics on packet transmission.

To update information on the page, click **Refresh**.



View list of currently associated client stations

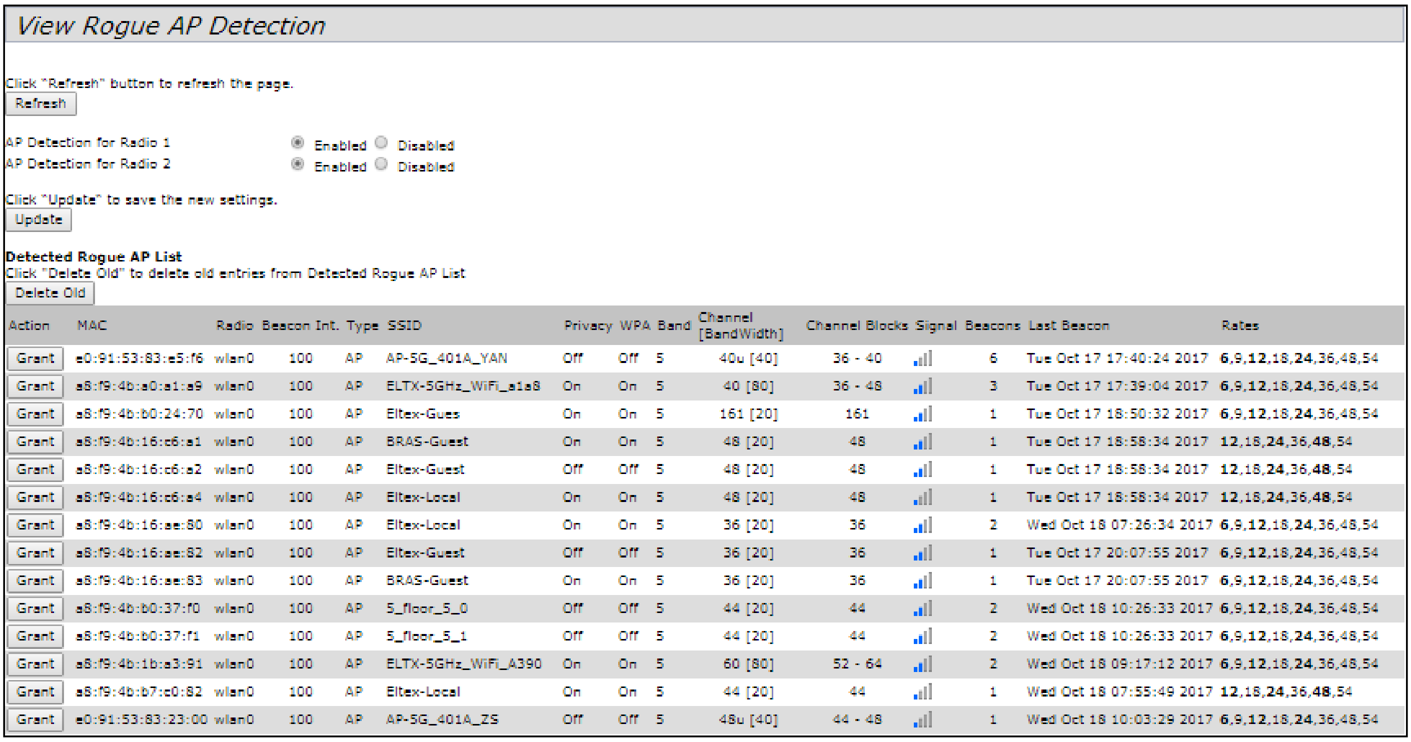
Click "Refresh" button to refresh the page.

Refresh

Total Number of Associated Clients 10

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capacity	Status Authorized
Eltex-Local (wlan0vap1)	24:a2:e1:0c:84:1a	192.168.40.189	iPad-Ksenia	00:00:00	-67	25 dB	-92 dBm	95%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	b4:9d:0b:5f:54:b9	192.168.40.89	android-538f33b42490714c	00:00:02	-62	30 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	20:a2:e4:e9:b1:c8	192.168.40.221	iPhone	00:00:13	-70	22 dB	-92 dBm	94%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	e0:63:e5:9a:b9:8d	192.168.40.203	android-6b261ba77ddb1eac	00:00:37	-72	20 dB	-92 dBm	98%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	34:ab:37:1c:0a:fc	192.168.40.67	Blackka-iPad	00:02:06	-48	44 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	8c:00:6d:44:99:9d	192.168.40.79	iMike	00:00:00	-44	48 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	00:0c:e7:90:de:95	192.168.40.215	android-d00406f9ec6a6e86	00:00:08	-60	32 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	70:8b:cd:72:b4:5e		android-b467ed42bdb068e6	00:00:06	-35	57 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	64:bc:0c:16:3a:b1	192.168.40.208	android-543291c57947a4fb	00:00:12	-64	28 dB	-92 dBm	50%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	20:e4:17:03:02:c3		stanislav-pc	00:00:20	-43	49 dB	-92 dBm	0%	Not supported	Not supported	Yes

In the **Rogue AP Detection** submenu, information about all wireless access points that the device detects in its network is displayed.



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.

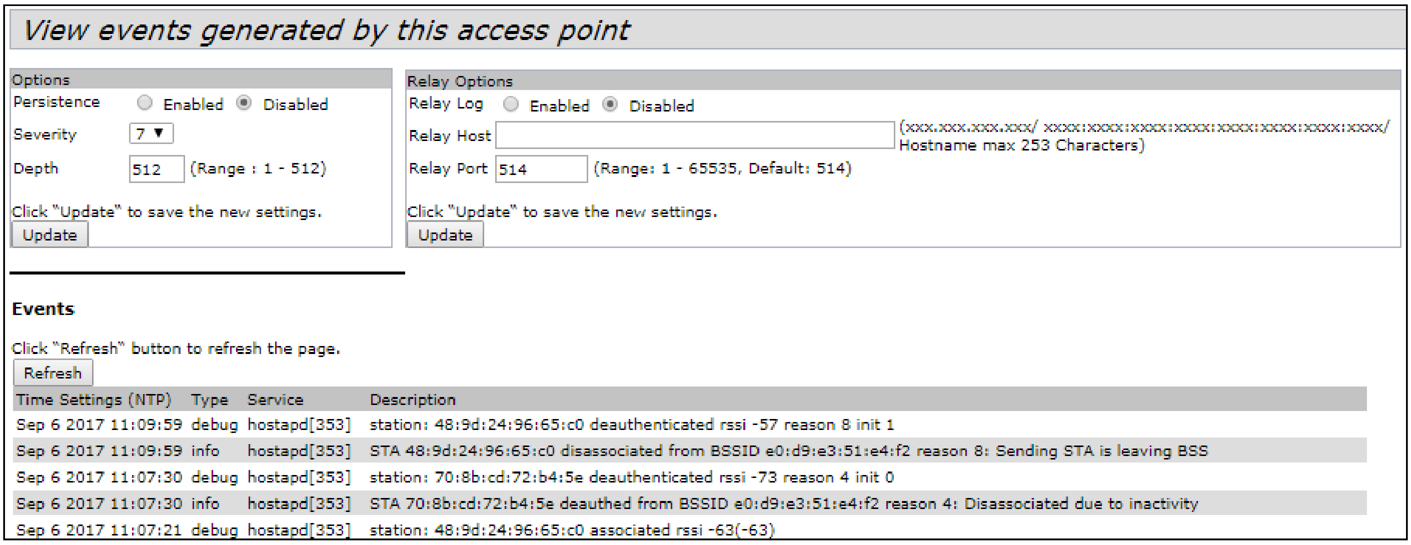
Update

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 [BandWidth]	Channel Blocks	Signal	Beacons	Last Beacon	Rates
Grant	e0:91:53:83:e5:f6	wlan0	100	AP	AP-5G_401A_YAN	Off	Off	5	40u [40]	36 - 40	📶	6	Tue Oct 17 17:40:24 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:a0:a1:a9	wlan0	100	AP	ELTX-5GHz_WiFi_a1a8	On	On	5	40 [80]	36 - 48	📶	3	Tue Oct 17 17:39:04 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b0:24:70	wlan0	100	AP	Eltex-Gues	On	On	5	161 [20]	161	📶	1	Tue Oct 17 18:50:32 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:16:c6:a1	wlan0	100	AP	BRAS-Guest	On	On	5	48 [20]	48	📶	1	Tue Oct 17 18:58:34 2017	**12**,18,**24**,36,**48**,54
Grant	a8:f9:4b:16:c6:a2	wlan0	100	AP	Eltex-Guest	Off	Off	5	48 [20]	48	📶	1	Tue Oct 17 18:58:34 2017	**12**,18,**24**,36,**48**,54
Grant	a8:f9:4b:16:c6:a4	wlan0	100	AP	Eltex-Local	On	On	5	48 [20]	48	📶	1	Tue Oct 17 18:58:34 2017	**12**,18,**24**,36,**48**,54
Grant	a8:f9:4b:16:ae:80	wlan0	100	AP	Eltex-Local	On	On	5	36 [20]	36	📶	2	Wed Oct 18 07:26:34 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:16:ae:82	wlan0	100	AP	Eltex-Guest	Off	Off	5	36 [20]	36	📶	1	Tue Oct 17 20:07:55 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:16:ae:83	wlan0	100	AP	BRAS-Guest	On	On	5	36 [20]	36	📶	1	Tue Oct 17 20:07:55 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b0:37:f0	wlan0	100	AP	5_floor_5_0	Off	Off	5	44 [20]	44	📶	2	Wed Oct 18 10:26:33 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b0:37:f1	wlan0	100	AP	5_floor_5_1	Off	Off	5	44 [20]	44	📶	2	Wed Oct 18 10:26:33 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:1b:a3:91	wlan0	100	AP	ELTX-5GHz_WiFi_A390	On	On	5	60 [80]	52 - 64	📶	2	Wed Oct 18 09:17:12 2017	**6**,**9**,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b7:c0:82	wlan0	100	AP	Eltex-Local	On	On	5	44 [20]	44	📶	1	Wed Oct 18 07:55:49 2017	**12**,18,**24**,36,**48**,54
Grant	e0:91:53:83:23:00	wlan0	100	AP	AP-5G_401A_ZS	Off	Off	5	48u [40]	44 - 48	📶	1	Wed Oct 18 10:03:29 2017	**6**,**9**,**12**,18,**24**,36,48,54

Events submenu displays a list of events that occur with the device, as well as configure event redirection to a third-party SYSLOG server.



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.

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.

Events

Click "Refresh" button to refresh the page.

Time Settings (NTP)	Type	Service	Description
Sep 6 2017 11:09:59	debug	hostapd[353]	station: 48:9d:24:96:65:c0 deauthenticated rssi -57 reason 8 init 1
Sep 6 2017 11:09:59	info	hostapd[353]	STA 48:9d:24:96:65:c0 disassociated from BSSID e0:d9:e3:51:e4:f2 reason 8: Sending STA is leaving BSS
Sep 6 2017 11:07:30	debug	hostapd[353]	station: 70:8b:cd:72:b4:5e deauthenticated rssi -73 reason 4 init 0
Sep 6 2017 11:07:30	info	hostapd[353]	STA 70:8b:cd:72:b4:5e deauthed from BSSID e0:d9:e3:51:e4:f2 reason 4: Disassociated due to inactivity
Sep 6 2017 11:07:21	debug	hostapd[353]	station: 48:9d:24:96:65:c0 associated rssi -63(-63)

For more detailed information, it is recommended to read the complete user manual.

10 Cluster operating mode

The cluster operation mode allows managing devices in a cluster simultaneously, which sufficiently improves operation efficiency while deploying, configuring or exploiting a wireless network.

When operating in Cluster mode, it is enough to configure only one access point. The rest of the access points will copy the configuration of the device with set parameters. If the configuration of one access point in a cluster has been changed, the other access points will apply the same changes. The solution is valid while firmware update. Operation in Cluster mode allows performing manageable consistent firmware update of devices in a cluster.

The cluster is a group of devices allocated in a single broadcast domain with synchronized configuration and firmware. Cluster mode is enabled by default.

The defining parameter of the mode is the name of a cluster by which the identification of device attachment to this cluster is performed. The default name of a cluster is default.

After loading, WEP-2ac defines if there are devices located on the network with the same name as in its configuration. If the devices with these parameters are not found, WEP-2ac becomes a master of the cluster. If the devices belonging to the cluster are found, WEP-2ac starts copying the configuration of a master. Thus, the first device with enabled Cluster mode occurred on the network becomes a master of its cluster. Other devices occurred on the network later and having the same cluster name start duplicating the master configuration. Several clusters with different names might be located in the same network simultaneously. One access point should be included to only one cluster.

WEP-2ac announces its affiliation to a cluster through a special protocol. The device sends broadcast UDP packets to LAN with data on affiliation to a particular cluster. Thus, all the access points included to a cluster exchange data among them, identify a master of the cluster and its configuration. The master carries out an inventory of the devices in the cluster and always controls the quantity of the access points in the cluster and their addresses.

Only access points from the same group can be combined into a cluster:

1 group	WEP-12ac	WOP-12ac			
2 group	WEP-2ac	WEP-2ac Smart	WOP-2ac	WOP-2ac SFP	WOP-2ac GPON

10.1 Installation

It is sufficient that only one access point is configured when deploying a network. For providing data exchange among devices in a cluster, install a DHCP server for network addresses distribution.
Network installation algorithm:

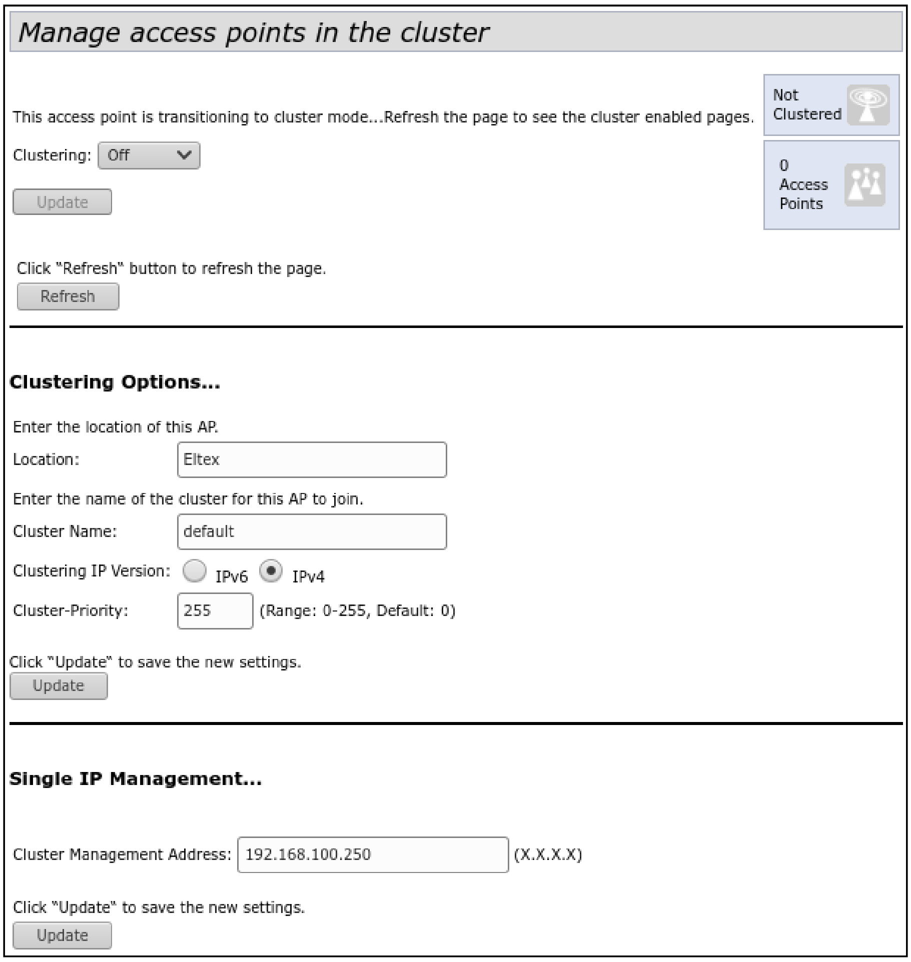
1. DHCP server installation;
2. Configuration and physical connection of one access point;
3. Physical connection of other access points in the cluster.

After installing the first access point, there is no need to configure the rest, it is sufficient to connect them physically to the network. The devices will obtain network addresses, define the master of the default cluster and will be automatically configured according to the master configuration.

10.2 Configuring Cluster

1. The device can work in a cluster only if WDS (Wireless Distribution System) and WGB (Work Group Bridge) are disabled.
2. To work in a Management cluster, the Ethernet interface of all points must be within the same network.
3. Cluster operating mode is disabled by default.

In the **Cluster** menu, open **Access Points** tab and perform the following:



Manage access points in the cluster

This access point is transitioning to cluster mode...Refresh the page to see the cluster enabled pages.

Clustering: Off

Click "Refresh" button to refresh the page.

Clustering Options...

Enter the location of this AP.

Location: Eltex

Enter the name of the cluster for this AP to join.

Cluster Name: default

Clustering IP Version: ○ IPv6 ● IPv4

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

Click "Update" to save the new settings.

Single IP Management...

Cluster Management Address: 192.168.100.250 (X.X.X.X)

Click "Update" to save the new settings.

To edit the settings in the **Clustering Options** section, switch cluster mode to **Off** state.

In the **Clustering Options** menu, perform the following configuration:

- *Location* – description of the physical location of the access point. Used to display in monitoring tables for easy analysis and network management;
- *Cluster Name* – cluster name. The access point will connect only to the cluster which name is specified in this parameter. By default – default;
- *Clustering IP Version* – version of the IP protocol used to exchange control information between cluster devices;
- *Cluster-Priority* – access point priority in the cluster. The parameter takes values from 0 to 255. The default is 0. Supported only for IPv4 networks. The master in the cluster is the point that has the highest cluster priority. If the parameter is not set, the access point with the lowest MAC address becomes the master point in the cluster.

To apply a new configuration and save setting to non-volatile memory, click **Update**.

In the **Single IP Management** menu, perform the following configuration:

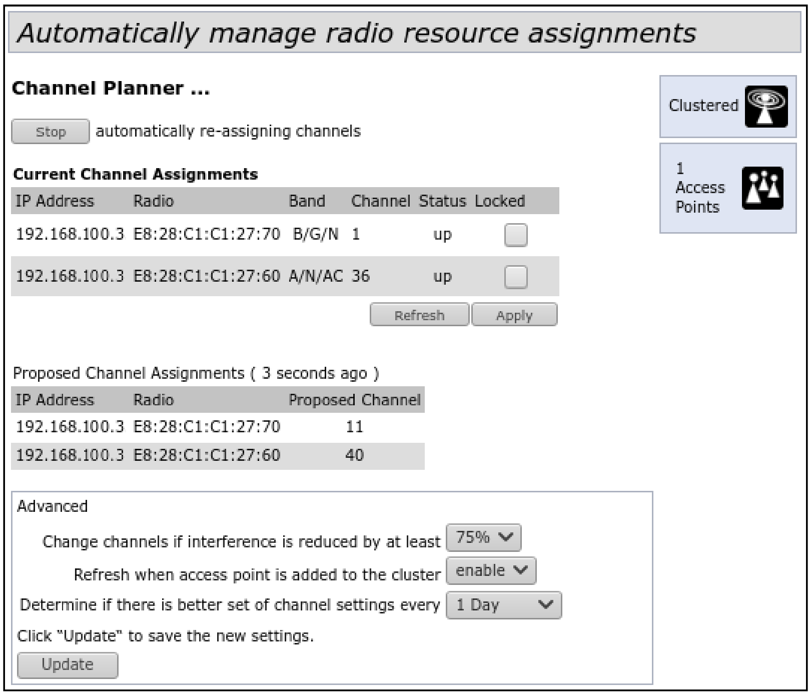
- *Cluster Management Address* – unique IPv4 address, at which the cluster master point will be available. This address must be on the cluster subnet and not be the same as the IP address of other devices on the network.

To apply a new configuration and save setting to non-volatile memory, click **Update**.

To enable cluster mode, select **On** in the **Clustering** field.

To enable automatic channel selection according to the data on channels used by neighboring access points and spectral analysis of environment on third-party access points noise, switch to the **Radio Resource Management** tab and click **Start** in the **Channel Planner** section.
To enable automatic output power distribution of the access point according to influence of neighboring access points which operate in the same cluster, switch to the **Radio Resource Management** tab and click **Start** in the **Transmit Power Control** section.

In the **Locked** field, channel change for the radio interface of the access point can be locked. If the flag is set when the optimal channel is selected by all access points, this radio interface will use the previous channel for any outcome of the optimal channel selection.



Automatically manage radio resource assignments

Channel Planner ...

Stop automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Status	Locked
192.168.100.3	E8:28:C1:C1:27:70	B/G/N	1	up	□
192.168.100.3	E8:28:C1:C1:27:60	A/N/AC	36	up	□

Refresh Apply

Proposed Channel Assignments (3 seconds ago)

IP Address	Radio	Proposed Channel
192.168.100.3	E8:28:C1:C1:27:70	11
192.168.100.3	E8:28:C1:C1:27:60	40

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 Day

Click "Update" to save the new settings.

Update

In the **Advanced** menu, perform the following configuration:

- *Change channels if interference is reduced by at least* – percentage gain in reducing the noise level for making a decision to switch to another channel. If, during the analysis of the environment, the access point detects that switching to another channel will result in a noise level decrease greater than the specified amount in this parameter, the decision will be made to switch to another channel. The value setting range for this parameter is between 5% and 75%;
- *Refresh when access point is added to the cluster* – recalculate the overall spectral structure of the environment and select the optimal channel for access points if a new access point joins the cluster;
- *Determine if there is better set of channel settings every* – time interval after which the overall spectral structure of the environment is recalculated and the optimal channel for access points is selected. **1 Day** is used in the example.

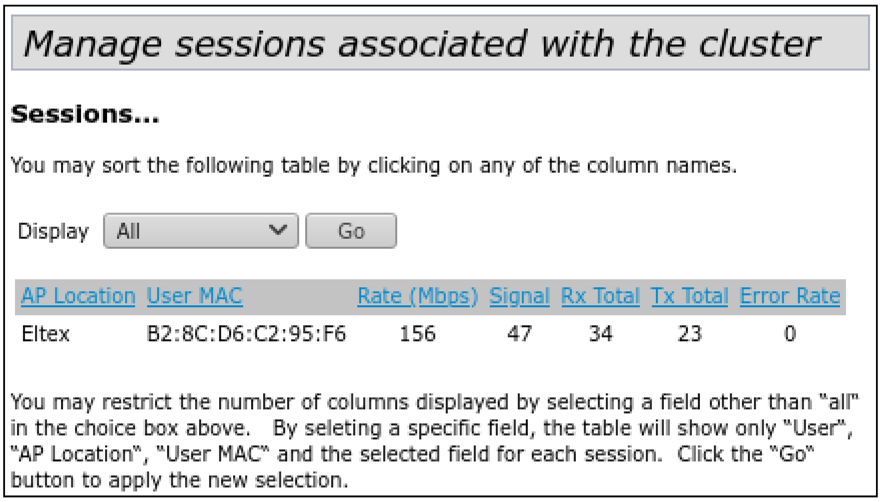
To apply a new configuration and save setting to non-volatile memory, click **Update**.

11 Monitoring

In the **Sessions** submenu, the parameters of client sessions connected to access points located in the cluster can be viewed. Each client is identified by the MAC address and access point to which it is currently connected.

To view statistics in the **Display** section, select the required value and click **Go.**

Statistics is available for the following parameters:



Manage sessions associated with the cluster

Sessions...

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

Display All Go

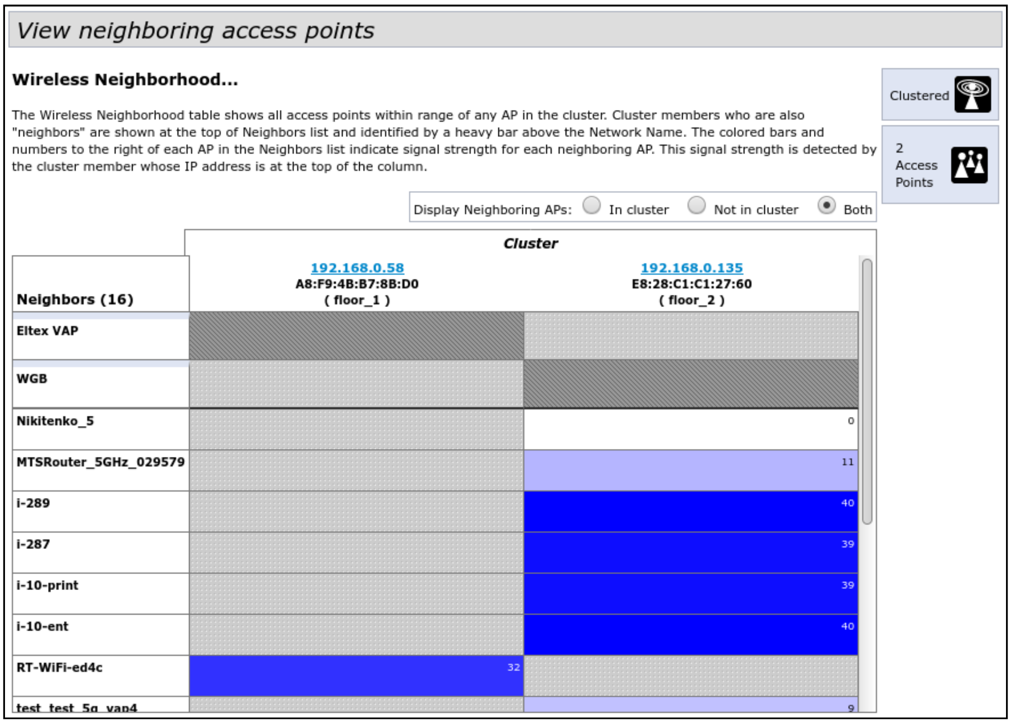
AP Location	User MAC	Rate (Mbps)	Signal	Rx Total	Tx Total	Error Rate
Eltex	B2:8C:D6:C2:95:F6	156	47	34	23	0

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.

- *AP Location* – description of the physical location of the access point;
- *User MAC* – MAC address of the client's wireless device;
- *Rate* – data transfer rate between the access point and a specific client, Mbps;
- *Signal* – signal level received from the access point;
- *Rx Total* – total number of packets received by the client during this session;
- *Tx Total* – total number of packets transmitted from the client during this session;
- *Error Rate* – percentage of resent packets.

To view correspondence between access points located in the cluster and wireless networks detected by these devices, switch to the **Wireless Neighborhood** tab.

In the **Wireless Neighborhood** tab,



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 (16)	192.168.0.58 A8:F9:4B:B7:8B:D0 (floor_1)	192.168.0.135 E8:28:C1:C1:27:60 (floor_2)
Eltex VAP		
WGB		
Nikitenko_5		0
MTSRouter_5GHz_029579		11
i-289		40
i-287		39
i-10-print		39
i-10-ent		40
RT-WiFi-ed4c	32	
test_test_5g_vap4		9

Based on this table, a spectral analysis of the entire network can be performed, and the impact of interference on each access point can be evaluated. This will enable the assessment of the correct location of access points across the coverage area and identification of problem areas where the level of interference may affect the quality of services.

The top line of the table displays information on each radio interface of access points located in the cluster. The far left column 'Neighbors' contains information on wireless networks that are visible to devices in the cluster.

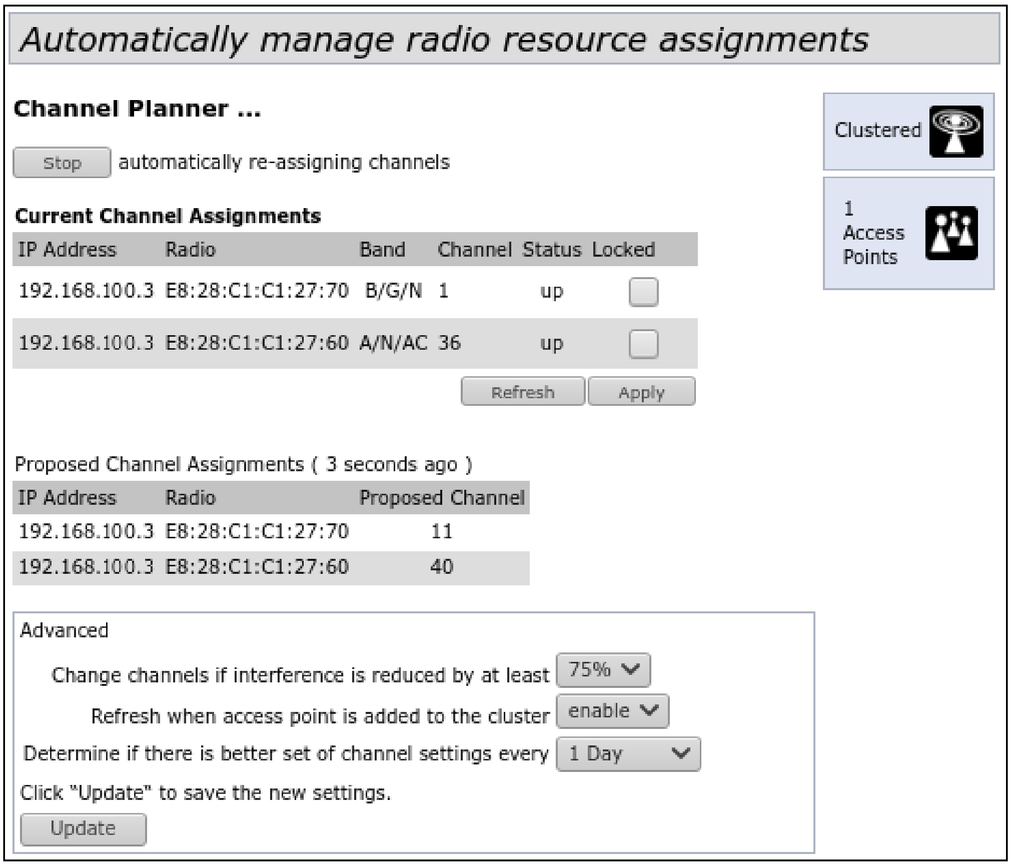
The signal level from each wireless network is indicated in the upper right corner of the table cell.

The table is formed in such a way that its first rows display wireless networks formed by the cluster itself, followed by the names of third-party networks.

To view current list of the access points in the cluster and their parameters, switch to the **Radio Resource Management** tab. In the **Current Channel Assignments** table, the following parameters are listed:

- *IP Address* – IP address of the access point in the cluster;
- *Radio* – MAC address of a radio interface of the access point in the cluster;
- *Band* – standards supported by the radio interface of the access point in the cluster at the moment;
- *Channel* – number of a channel on which the access point operate;
- *Status* – operation state of the access point’s radio interface in the cluster;

To update information on the page, click **Refresh**.



Automatically manage radio resource assignments

Channel Planner ...

Stop automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Status	Locked
192.168.100.3	E8:28:C1:C1:27:70	B/G/N	1	up	□
192.168.100.3	E8:28:C1:C1:27:60	A/N/AC	36	up	□

Proposed Channel Assignments (3 seconds ago)

IP Address	Radio	Proposed Channel
192.168.100.3	E8:28:C1:C1:27:70	11
192.168.100.3	E8:28:C1:C1:27:60	40

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 Day

Click "Update" to save the new settings.

The **Proposed Channel Assignments** table contains data on available channel values, which the radio interface will switch to if optimal channel selection has been launched:

- *IP Address* – IP address of the access point in the cluster;
- *Radio* – MAC address of a radio interface of the access point in the cluster;
- *Proposed Channel* – channel number to which the radio interface will switch when optimal channel selection is launched.

11.1 Cluster firmware upgrade

The operation in the cluster mode allows performing automatic firmware upgrade for all the access points in the cluster without using external systems or controllers.

Firmware upgrade might be performed:

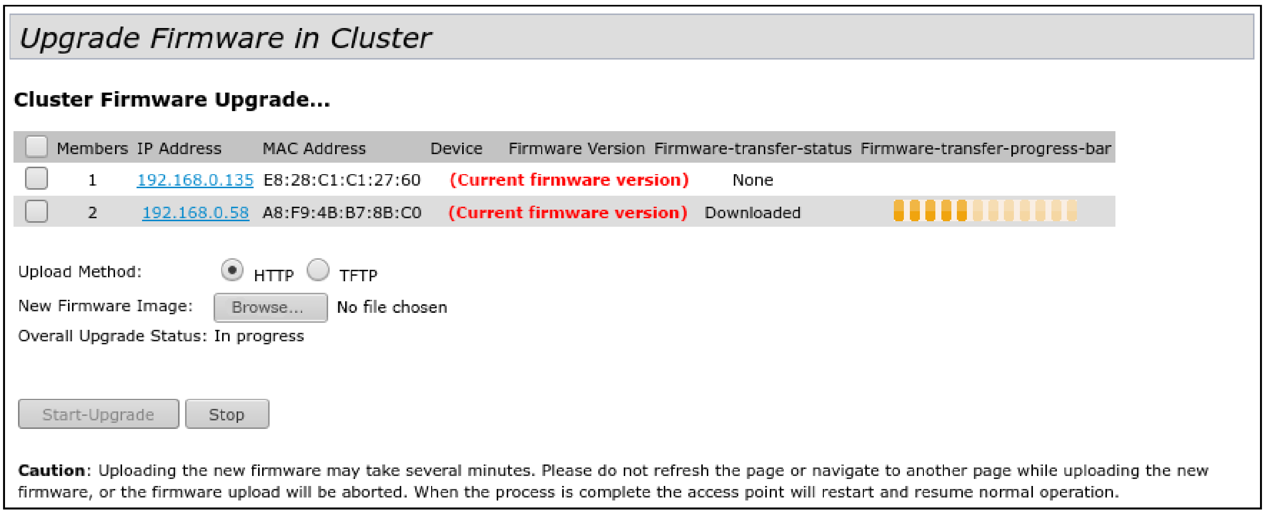
- through the web interface;
- through the DHCP Autoprovisioning (opt 66, opt 67).

11.1.1 Firmware upgrade via web interface

To upgrade firmware on devices in a cluster through web interface, open the **Cluster Firmware Upgrade** tab of an access point.

When updating the firmware of the cluster devices, the firmware file will be downloaded to each device and set to the 'Primary Image' position. The upgrade process automatically reboots devices with firmware that matches the new image. The firmware installed earlier on the cluster devices will be saved and moved to the 'Secondary Image' position (backup version of the firmware).

Download the file with the current firmware version to PC.



Upgrade Firmware in Cluster

Cluster Firmware Upgrade...

□	Members	IP Address	MAC Address	Device	Firmware Version	Firmware-transfer-status	Firmware-transfer-progress-bar
□	1	192.168.0.135	E8:28:C1:C1:27:60		(Current firmware version)	None	
□	2	192.168.0.58	A8:F9:4B:B7:8B:C0		(Current firmware version)	Downloaded	▮▮▮▮▮▯▯▯▯▯▯▯

Upload Method: ● HTTP ○ TFTP

New Firmware Image: Browse... No file chosen

Overall Upgrade Status: In progress

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 firmware file can be uploaded to the device via HTTP or TFTP protocols:

Upload via HTTP. Set **Upload Method** flag to HTTP. Click **Browse**. In the window that opens select a path to the firmware file on the PC. In the leftmost column of the table, set flags for access points for which firmware will be upgraded. Click **Start-Upgrade** to start upgrading.

Upload via TFTP. Set **Upload Method** flag to TFTP. In the **Image Filename** field specify the name of the firmware file that will be uploaded to the device. File name must contain .tar extension. In the **Server IP** field specify the IP address for the TFTP server on which the firmware file will be stored.

Click **Stop** to abort device upgrade process.

In the **Overall Upgrade Status** field, a summary status of the software upgrade process on access points is displayed.

While updating the device firmware, do not turn off the power of the device, and do not update or change the current web page with the update progress bar.

11.1.2 Firmware upgrade via DHCP Autoprovisioning

To upgrade firmware, a TFTP server and a DHCP server with particular configuration are required. The upgrade process is as follows:

1. An access point is loaded and obtains address via DHCP. The access point obtains 2 parameters from the server while DHCP session: tftp-server and file name, where tftp-server – an IP address of TFTP server, and filename is a name of the file with .manifest extension which contains data on the firmware.
2. A master of the cluster, according to received data, starts make attempts to download manifest-file from TFTP server. After downloading the file, the master compares firmware version specified in a file with its own. If firmware versions are different, the master downloads firmware file from the TFTP server (file name of the firmware is specified in manifest-file) and updates automatically.
3. The other devices in the cluster define that the master is not in operation. Then, new master is selected in the cluster. The device with bigger uptime value becomes a master. New master also repeat the second step: downloads manifest-file, compares firmware versions and updates.
4. The cycle is repeated until all the devices in the cluster are upgraded.

11.1.3 Firmware upgrade algorithm via DHCP Autoprovisioning

1. Place the 'wep2.manifest' file on TFTP server, the file should contain the following string:

```
VERSION= '1.22.X.X' WEP-2ac-1.22.X.X.tar.gz,
```

where WEP-2ac-1.22.X.X.tar.gz is a name of the archive containing firmware for WEP-2ac;
1.22.X.X is a firmware version included to the archive. The firmware version can be viewed in 'version' file in firmware archive.

2. Place archive with firmware for WEP-2ac on TFTP server.

3. Add the following strings to the DHCP server configuration file (dhcpd.conf):

```
option tftp-server-name '192.168.100.253';
option bootfile-name 'wep2.manifest';
```

where 192.168.100.253 is an address of the TFTP server;
wep2.manifest is a manifest file name.

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

http://www.eltex-co.com/support

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist in our technical forum.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/