# ELTEX

Wireless access point

# WOP-2ac

Quick guide

Firmware version 1.20.0

IP address: 192.168.1.10
Username: admin
Password: password

Contents

# 1 Annotation

This manual specifies the following:

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

The manual gives an example of access point configuration without using a soft controller.
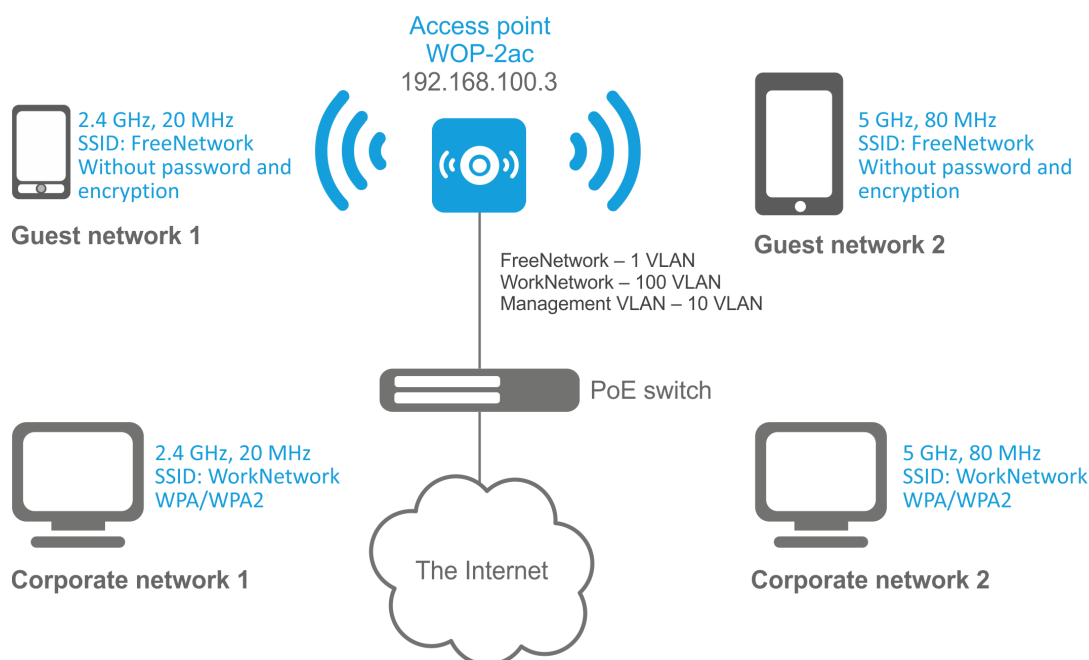
The following scheme is given as an example:

Access point
WOP-2ac
192.168.100.3

2.4 GHz, 20 MHz
SSID: FreeNetwork
Without password and
encryption

**Guest network 1**

5 GHz, 80 MHz
SSID: FreeNetwork
Without password and
encryption

**Guest network 2**

FreeNetwork – 1 VLAN
WorkNetwork – 100 VLAN
Management VLAN – 10 VLAN

PoE switch

2.4 GHz, 20 MHz
SSID: WorkNetwork
WPA/WPA2

**Corporate network 1**

The Internet

5 GHz, 80 MHz
SSID: WorkNetwork
WPA/WPA2

**Corporate network 2**

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, you need to have PC with access to the device via Ethernet and any web browser (Internet Explorer, Firefox, Google Chrome, Opera, etc.)

## 2  Connecting the web interface

Connection of PC to the device might be executed as follows:

- Connect network cable to PoE interface of WOP-2ac and to PoE injector (or switch). Then connect a PC to the PoE injector (or switch).

To connect to the web interface of the device, enter the following to the URL bar of your browser: **192.168.1.10.**
If the connection has been performed successfully, the authorization page will be displayed. Use the following data for authorization:

- **User Name: admin**
- **Password: password**

If the authorization page is not displayed after entering the device IP in the browser, check the IP address on the PC and switch settings. If the configuration on the device has been changed (is not a default one), reset the device to factory settings. To perform this, press and hold the button «F» on the side panel of the device within 20 seconds.

# 3  Configuration of WOP-2ac network parameters

For remote management of WOP-2ac, you should 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                        WOP-2ac              (Range : 1 - 63 characters)

Internal Interface Settings
MAC Address                     A8:F9:4B:B7:ED:60
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 . 15 . 250
Subnet Mask                     255 . 255 . 255 . 0
Default Gateway                 192 . 168 . 15 . 1
DNS Nameservers                 ○ Dynamic ● Manual
                                    .     .     .
                                    .     .     .

Click "Update" to save the new settings.
 Update
```

- **Management VLAN ID** – set the number of VLAN that you are going to use for access point management. 1 is used in the given example.
- **Connection Type** – select «Static IP» to set IP addresses for access points manually. Specify the IP address of WOP-2ac (in the example, it is 192.168.15.250) in the **«Static IP Address»** Enter the address of the default gateway in the **«Default Gateway»** field. 192.168.15.1. Changing the network mask is optional. If you want the access points to obtain IP addresses via DHCP, «Connection type» field should be set to «DHCP» value. If DHCP is selected, the network settings configuration is completed.

Click **«Update»**. Since that, WOP-2ac is available in 1 VLAN via 192.168.15.250 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, you may undo them by resetting the access point to factory settings. To perform 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.

# 4  WOP-2ac firmware update

For proper operation of WOP-2ac, it is recommended to update the firmware. You may consult the vendor on the relevance of the firmware version:

e-mail: **techsupp@eltex.nsk.ru**
After obtaining the relevant firmware version, open the menu **«Maintenance»**, **«Upgrade»** tab and perform the following:



- Press **«Switch»** button if you want to switch to an Alternative firmware image set in **«Secondary Image»**
- **Upload Method** – check **«HTTP»**
- **New Firmware Image** – click **«Browse»** button and select relevant firmware version, click **«Open»**.

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 update is completed.

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

You may check the current firmware version in the **«Basic Settings»** menu (Firmware Version)**.**

## Provide basic settings

### ▌ Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address:        192.168.40.26
MAC Address:       E0:D9:E3:71:F5:40
Firmware Version:  1.12.0.286
Uptime:            9 days, 20 hours, 48 minutes
CPU Usage:         22.20%
Memory Usage:      130MB/248MB (52%)

[ Refresh ]

---

### 2 Device Information

Product Identifier:  WLAN-EAP
Hardware Version:    2v2
Serial Number :      WP12008615
Device Name:         Eltex-AP
Device Description:  WEP-2ac

---

### 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     [ WEP-26              ]
System Contact  [ admin@example.com   ]
System Location [ Default             ]

Click "Update" to save the new settings.
[ Update ]

# 5  SNMP service configuration

SNMP service configuration is performed in the **«Services»** menu, **«SNMP»** section.

**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 ▼ | | |

**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.
[Update]

- **Restrict the source of SNMP requests to only the designated hosts or subnets – check the** «Enabled» **box**.
- **Hostname, address, or subnet of Network Management System** – specify an IP-address of SNMP server, from which SNMP commands will be transmitted.
- **Community name for traps** – set **«public»**.
- **Enabled/Host Type/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 WOP-2ac will send traps.
- Click **«Update»**.

# 6 Wireless interfaces configuration

WOP-2ac has 2 radio interfaces which are capable to operate simultaneously – Radio 1 and Radio 2. Each interface is capable to operate on its frequency band in different wireless network modes.
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: 40 MHz.

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



- **Country** – select settings according to the rules of selected country. Select **«Russia»** in the list.
- **Transmit Power Control** – configuring *Transmit Power Limit* parameter restrictions. Select **«On»** in the list.

Configuring Radio 1:

- **Radio Interface 2** – check the **«On»**
- **Mode** – select the **«IEEE 802.11a/n/ac»** value;
- Click **«Update»**.

Configuring Radio 2:

- **Radio Interface** – check the **«On»**
- **Mode** – select the **«IEEE 802.11b/g/n»**

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.
[ Update ]

Configuring Radio 1:

- **Radio** – select the «**1**»
- **Channel Bandwidth** – set the «**80MHz**»
- Click «**Update**».

Configuring Radio 2:

- **Radio** – select the «**2**»
- **Channel Bandwidth** – set the «**40MHz**»
- Click «**Update**».

# 7 Virtual access points configuration

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

Band Steer feature allows clients having opportunity of operation at 2.4 GHz and 5 GHz to set priority of connection to  virtual access points operating at 5 GHz.
The followings are necessary for Band Steer feature operation:

- configure radio interfaces for different frequency ranges;
- create virtual access points (VAP) with the same SSID on each radio interface;
- make sure that the passwords on the access points are the same if you use encryption;
- Activate Band Steer parameter on access points.

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



Configuring Radio 1:

- **Radio** – select the **«1»**
- **Enabled** – check the boxes for VAP 0 and VAP1.
- **VLAN ID** – VLAN number:
    - set value **«100»** for VAP 0;
    - set value **«1»** for VAP 1.
- **SSID** – wireless network name:
    - set value **«WorkNetwork»** for VAP 0;
    - set value **«FreeNetwork»** for VAP 1.
- **Station Isolation** – forbid packet transmission among access point's clients. Check the box.
- **Band Steer** – set a priority of users connection to SSID configured at 5 GHz. Check the box.
- **VLAN Priority** – the 2nd priority level which will be assigned to packets transmitted through the given VAP from radio environment to wired network.
- **Security** – secure network mode:
    - set **«WPA Personal»** value for VAP 0 and set a password for this network connection in the **«Key»** field;
    - set value **«None»** for VAP 1.
- Click **«Update»**.

Configuration of Radio 2 is performed in the same way. Select **«2»** value in **Radio** and perform the configuration as for the Radio 1 (given above). The password for «WorkNetwork» should be the same. Click **«Update»**.

> ✅ When using WPA Enterprise mode, the authorization is implemented through a RADIUS server. The request on user connection to SSID is sent to a RADIUS server. The table *Global RADIUS server settings* specifies the following:
> - RADIUS IP Address – an IP address of a RADIUS server;
> - RADIUS Key – a password to access the RADIUS server.

# 8  Monitoring main parameters of wireless network

You may view the list of connected users in the **«Status»** menu, **«Client Association»** tab.

```
View list of currently associated client stations

Click "Refresh" button to refresh the page.
Refresh

Total Number of Associated Clients  0

Network Station Hostname Status    From Station                                  To Station
                        Authorized Packets Bytes Drop Packets Drop Bytes TS Violate Pkts  Packets Bytes Drop Packets Drop Bytes TS Violate Pkts
```

The list of third-party access points in WOP-2ac area with data on wireless channel used and transmitted signal level is presented in the **«Status»** menu, **«Rogue AP Detection»** tab.

```
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 | a8:f9:4b:b2:2d:74 | wlan0 | 100 | AP | ASM | Off | Off | 5 | 48 [20] | 48 | | 10 | Wed Sep 6 11:31:56 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b1 | wlan0 | 100 | AP | Eltex-Local | On | On | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 12:38:05 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b2 | wlan0 | 100 | AP | Eltex-Guest | Off | Off | 5 | 48 [20] | 48 | | 5 | Wed Sep 6 11:49:08 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b4 | wlan0 | 100 | AP | BRAS-Guest | On | On | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 11:28:46 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:1f:fc:90 | wlan0 | 100 | AP | OpenPortal | Off | Off | 5 | 44 [20] | 44 | | 5 | Wed Sep 6 20:22:23 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b0 | wlan0 | 100 | AP | (Non Broadcasting) | Off | Off | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 12:38:05 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:d9:c9:b9 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_C9B8 | On | On | 5 | 52 [80] | 52 - 64 | | 6 | Wed Sep 6 14:06:49 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:dc:f8:02 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_F800 | On | On | 5 | 36 [80] | 36 - 48 | | 4 | Wed Sep 6 14:19:55 2017 | 6,9,12,18,24,36,48,54 |
| Grant | e0:d9:e3:6b:e0:7a | wlan0 | 100 | AP | ELTX-5GHz_WiFi_E078 | On | On | 5 | 52 [80] | 52 - 64 | | 4 | Wed Sep 6 14:06:49 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:e3:15:51 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_1550 | On | On | 5 | 36 [80] | 36 - 48 | | 3 | Wed Sep 6 17:11:36 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:e3:16:69 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_1668 | On | On | 5 | 56 [80] | 52 - 64 | | 3 | Wed Sep 6 11:33:17 2017 | 6,9,12,18,24,36,48,54 |

The list of events is given in the **«Status»** menu, **«Events»** tab.

```
View events generated by this access point

Options                                    Relay Options
Persistence      ○ Enabled ◉ Disabled      Relay Log   ○ Enabled ◉ Disabled
Severity         7 ▼                        Relay Host  [                    ]  (xxx.xxx.xxx.xxx/ xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/
                                                                                Hostname max 253 Characters)
Depth            512  (Range : 1 - 512)     Relay Port  514   (Range: 1 - 65535, Default: 514)

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


Events

Click "Refresh" button to refresh the page.
Refresh
```

| Time Settings (NTP) | Type | Service | Description |
|---|---|---|---|
| Sep 8 2017 10:06:16 | info | hostapd[1732] | AP with MAC address e0:36:76:61:c3:74 and SSID PLDTHOMEFIBR_CARPIO is detected on channel 11 |
| Sep 8 2017 10:05:16 | info | hostapd[1732] | AP with MAC address a8:f9:4b:ba:64:9a and SSID Orion2.4 is detected on channel 11 |
| Sep 8 2017 09:57:57 | info | login[1186] | root login on 'ttyS0' |
| Sep 8 2017 09:56:12 | info | hostapd[1732] | AP with MAC address a8:f9:4b:b0:2d:a0 and SSID wop-2_test is detected on channel 1 |
| Sep 8 2017 09:55:46 | info | clusterd[1845] | AP with MAC Address "A8:F9:4B:B7:ED:60" and priority "0" is elected as Dominant AP |
| Dec 31 1999 12:00:36 | info | dman[1178] | DHCP-client: Interface brtrunk ip changed |

To obtain more detailed information, read the full user manual.

# 9 Cluster operation mode

## 9.1 Description

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

When operating in Cluster mode, it is sufficiently that you 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 to perform 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, WOP-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, WOP-2ac becomes a master of the cluster. If the devices belonging to the cluster are found, WOP-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.

WOP-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.

## 9.2 Installation

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

Network installation algorithm:

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

After installing the first access point, you do not 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 Cluster configuration

✅ The device may operate in a cluster only if WDS (Wireless Distribution System) and WGB (Work Group Bridge) features are disabled.

✅ For operation in a cluster Management Ethernet interfaces of all access points should be located in one network.

✅ Cluster operation mode is disabled by default.

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



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

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

- **Location** – specify physical location of the access point. The option is used to analyse and control the network in different monitoring tables. *«Eltex»* is used in the example;
- **Cluster Name** – set name cluster. The access point will be connected only to a cluster, which name is specified in *«Cluster Name»*. *«default»* is used in the example;
- **Clustering IP Version** – select used IP version for management data exchange among access points in the cluster. *«IPv4»* is used in the example.
- **Cluster-Priority** – set the priority of the device in the cluster. *«0»* is used in the example.

Click **«Update»** to save changes.

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

- **Cluster Management Address** – specify an address via which the device may access the master cluster. The master should be located in the same subnet with the cluster. *«192.168.10.10»* is used in the example.

Click **«Update»** to save changes.

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



To enable automatic channel selection according to the data on channels used by neighbouring 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 neighbouring access points which operate in the same cluster, switch to the **«Radio Resource Management»** tab and click **«Start»** in the **«Transmit Power Control»** section.

### Automatically manage radio resource assignments

**Channel Planner ...**

Start | automatically re-assigning channels

**Current Channel Assignments**

| IP Address | Radio | Band | Channel | Status |
|---|---|---|---|---|
| 192.168.15.129 | A8:F9:4B:B7:ED:70 | B/G/N | 1 | up |
| 192.168.15.129 | A8:F9:4B:B7:ED:60 | A/N/AC | 36 | up |

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]

**Transmit Power Control ...**

Start | automatically re-assigning tx power

| | | |
|---|---|---|
| RSSI threshold 2.4 GHz | -65 | (Range: -100...-30) |
| RSSI threshold 5 GHz | -70 | (Range: -100...-30) |
| Interval | 0 | (Range: 1800...86400 or 0) |

Advanced

| | | |
|---|---|---|
| Minimal Tx Power | 10 | (Range: 6...30) |
| Active Scan Mode | ☑ | |
| Debug Mode | ☐ | |

[Update]

Monitoring   [Expand]

TPC statistics is not available because tpc-planner is not up

Clustered 📡

1 Access Points 👥

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

- **Change channels if interference is reduced by at least** – select a percentage that the interference must be reduced by for the access point to change channels. *«75%»* is used in the example;
- **Refresh when access point is added to the cluster** – enable re-counting of common spectral structure of environment and selection of optimal channel for the access point (**«enable»** value) when new access point is being connected to the cluster.
- **Determine if there is better set of channel settings every** – set a time interval to schedule updates of environment spectral structure determination and selection of better channel for the access points. *«1Day»* is used in the example.

Click **«Update»** to save changes.

## 10.1  Monitoring

To view sessions parameters of clients connected to the access points of given cluster, switch to the **«Sessions»** tab.

Clients are defined through MAC addresses and an access points which they are connected to.

To view the statistics, select necessary value and click **«Go»** in the **«Display»** section. The following parameters might be viewed:



- **AP Location** – access point's location. The value is obtained from location description on the **«Basic Settings»** tab;
- **User MAC** – MAC address of client's wireless device;
- **Idle** – average time that the device has been in stand-by mode (when the device does not receive or transmit data);
- **Rate** – transmit data rate between an access point and a particular client, in Mbps;
- **Signal** – a level of signal received from an access point;
- **Rx Total** – total number of packets received by a client within current session;
- **Transmit Total** – total number of packets transmitted by a client within current session;
- **Error Rate** – total number of packets dropped by an access point within current session;

To view correspondence of access points in a cluster and wireless networks detected by these devices, switch to the **«Wireless Neighborhood»** tab. There is a table, on the **«Wireless Neighborhood»** tab, that shows which wireless networks are detected by each access point and what signal level each access point accept.

According to this table, spectral analysis of the whole network might be carried out and there is an opportunity to estimate interference influence to each access point. It will help you to estimate better location of access points among coverage area and to define locations with exceeding level of noise. The top string of the table contains data on each radio interface of access points included in a particular cluster. The left column contains data on wireless networks which are defined by the devices in the cluster. A value of signal level of each access point is displayed in the top-right cell of the table.

The table is formed in the way that wireless networks organized by a cluster are displayed first, the third-party networks follow after them.

The table might be displayed in 3 modes:

- **In cluster** – when checked, the table consists data only on wireless networks organized by the cluster;
- **Not in cluster** – when checked, the table consists data only on third-party wireless networks;
- **Both** – when checked, the table consists data on all wireless networks.

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

- **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;
- **Locked** – block channel change. When checked, the radio interface will always use the same channel even when another channel is selected as optimal for all the access points in the cluster.

Click «**Refresh**» to update the table «**Current Channel Assignments**».

The table **«Proposed Channel Assignments»** 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** – a channel number to which the radio interface will switch when optimal channel selection is launched.

## 10.2 Firmware update

The operation in the cluster mode allows to perform automatic firmware update for all the access points in the cluster without using external systems or controllers.
Firmware update might be performed:

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

### 10.2.1 Firmware update via web interface

To update firmware on devices in a cluster through web interface, open the **«Cluster Firmware Upgrade»** tab of an access point.
When updating firmware of devices in a cluster, the firmware file will be loaded to each access point and set to *«Primary Image»*. Reloading of the devices with new firmware version loading is performed automatically. The previous firmware version will be saved as *«Secondary Image»* (backup firmware version).
Perform the following in the **«Cluster Firmware Upgrade»** tab:
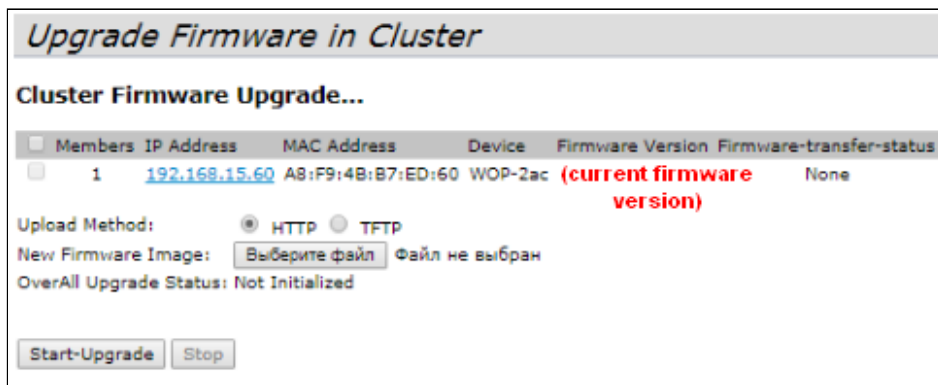
- **Upload Method** – select the firmware loading method for the devices. The loading through TFTP is used in the example:
- **Image Filename** – enter a file name of firmware which will be loaded to the device;
- **Server IP** – enter an IP address of TFTP server on which firmware file is saved. *«192.168.15.92»* is used in the given example.

Click **«Start-Upgrade»** to start updating.
While firmware updating, do not switch off the devices and do not update or change the web page with progress bar.


### 10.2.2 Firmware updating through DHCP Autoprovisioning

To update firmware, you need a TFTP server and a DHCP server with particular configuration. The updating 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 updated.

**Update configuration algorithm:**

1. Place the **"wop2.manifest"** file on TFTP server, the file should contain the following string:

   **VERSION= "1.20.0.X"WOP-2ac-1.20.0.X.tar.gz**,

   Where:
   WOP-2ac-1.20.0.X.tar.gz – name of the archive containing firmware for WOP-2ac;
   1.20.0.X – a firmware version included to the archive.
   The firmware version might be viewed in «version» file in firmware archive.

2. b) Place archive with firmware for WOP-2ac on TFTP server.
3. c) Correct DHCP server settings (dhcpd.conf) as follows:

   option tftp-server-name '192.168.10.1';
   option bootfile-name 'wop2.manifest';

   Where:

where 192.168.10.1 – an address of TFTP server;
manifest – manifest-name of the file.

# 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/