

Wireless access point

WOP-12ac

Quick guide

Firmware version 1.20.0

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1	Annotation.....	3
2	Connecting the web interface	4
3	Configuration of WOP-12ac network parameters	5
4	WOP-12ac firmware update	6
5	SNMP service configuration.....	7
6	Wireless interfaces configuration	8
7	Virtual access points configuration	10
8	Monitoring main parameters of wireless network	13
9	Cluster operation mode.....	15
9.1	Description	15
9.2	Installation	15
9.3	Cluster configuration	15
9.4	Monitoring	19
9.5	Firmware update.....	21
9.5.1	Firmware update via web interface	21
9.5.2	Firmware updating through DHCP Autoprovisioning	21

1 Annotation

This manual specifies the following:

- connection to WOP-12ac web interface;
- configuration of WOP-12ac network parameters;
- WOP-12ac 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.

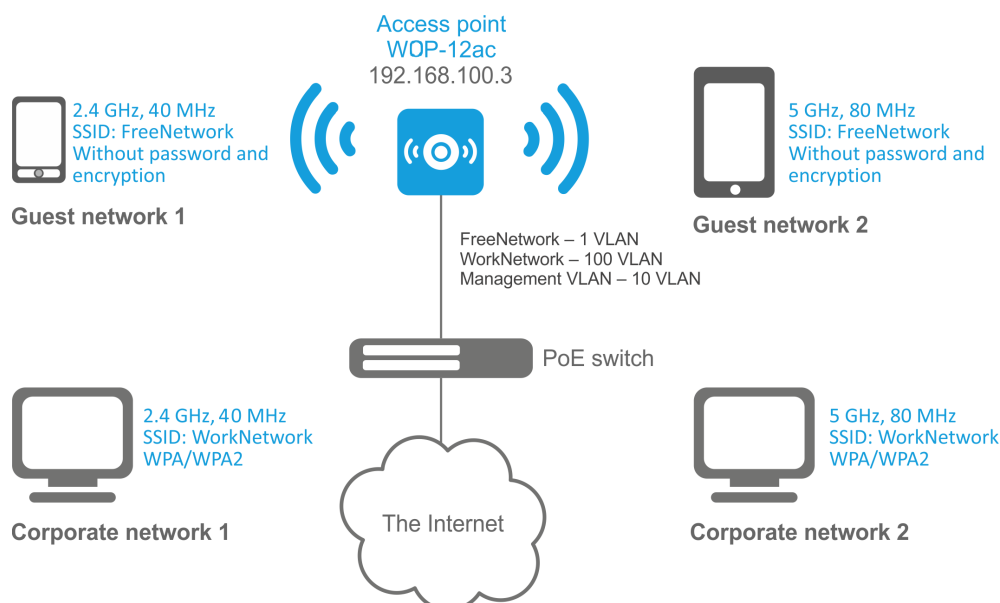


Figure 1 – Example of network configuration

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-12ac and to PoE injector (or switch). Then connect a PC to the PoE injector (or switch).
- You may connect WOP-12ac to 48VDC power source (optionally included in the delivery package) and connect a PC through 1 Ethernet interface of WOP-12ac.

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.

- 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-12ac network parameters

For remote management of WOP-12ac, 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 (Range : 1 - 63 characters)

Internal Interface Settings

MAC Address A8:F9:4B:B0:B5:40

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

Untagged VLAN ☒ Enabled ☐ Disabled

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

Connection Type

Static IP Address . . .

Subnet Mask . . .

Default Gateway . . .

DNS Nameservers ☐ Dynamic ☒ Manual

. . .

. . .

Click "Update" to save the new settings.

- **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-12ac (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-12ac 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-12ac firmware update

For proper operation of WOP-12ac, 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 «**Maintenance**» menu, «**Upgrade**» tab and perform the following:

- Click the «**Switch**» button if you want to switch to an Alternative firmware image set in the «**Secondary Image**»
- **Upload Method** – check «**HTTP**»
- **New Firmware Image** – click the «**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).

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) (Range: 1 - 256 characters)

Port number the SNMP agent will listen to (Range: 1025 - 65535, Default: 161)

Allow SNMP set requests ☒ Enabled ☐ Disabled

Read-write community name (for permitted SNMP set operations) (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)
<input type="checkbox"/>	IPv4	snmpV2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	IPv4	snmpV2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	IPv4	snmpV2	<input type="text"/>	<input type="text"/>

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

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

Logs priority level (for Standard output, Standard error and File logs output)

Logs priority range From to (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** – 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-12ac will send traps.
- Click «Update».

6 Wireless interfaces configuration

WOP-12ac 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: 2.4 GHz;
- Standards: 802.11b/g/n;
- Bandwidth: 40 MHz.

Radio2:

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

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: A8:F9:4B:B0:B5:40

Mode: IEEE 802.11b/g/n

Channel: Auto

Airtime Fairness: ☒ On ☐ Off

FBWA: ☐ On ☒ Off

Radio Interface 2 ☒ On ☐ Off

MAC Address: A8:F9:4B:B0:B5:50

Mode: IEEE 802.11a/n/ac

Channel: Auto

Airtime Fairness: ☒ On ☐ Off

FBWA: ☐ On ☒ Off

AeroScout™ Engine Protocol Support: Disabled

Click "Update" to save the new settings.

Update

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

Configuring Radio 2:

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

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

Modify radio settings

Radio 1 ▼

Status
☒ On
☐ Off

Mode
IEEE 802.11b/g/n ▼

Channel
Auto ▼

Channel Update Period
Off ▼

Limit Channels

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13	All
Use	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Channel Bandwidth
20 MHz ▼

Primary Channel
Lower ▼

Transmit Power Limit
16 (dBm, Range: 10 - 16)

Transmit Chain
☒ A1
☒ A2
☒ A3

Advanced Settings
+

TSPEC Settings
+

Click "Update" to save the new settings.

Update

Configuring Radio 1:

- **Radio** – select the «1»
- **Channel Bandwidth** – set value «40MHz».
- Click «**Update**».

Configuring Radio 2:

- **Radio** – select the «2»
- **Channel Bandwidth** – set value «80MHz».
- 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 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:

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	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="Work Network"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="WPA Personal"/>	<input type="text" value="Disabled"/>
<div>WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES</div> <div>Key: <input type="text" value="*****"/></div> <div>Broadcast Key Refresh Rate: <input type="text" value="0"/> (Range: 0-86400)</div>														
1	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="Free Network"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="None"/>	<input type="text" value="Disabled"/>
2	<input type="checkbox"/>	<input type="text" value="2600"/>	<input type="text" value="_Enterprise"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="WPA Enterprise"/>	<input type="text" value="Disabled"/>

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 «**Work Network**» for VAP 0;
 - set value «**Free Network**» 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 «Work Network» 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.

Modify Virtual Access Point settings

Global RADIUS server settings

RADIUS Domain:

RADIUS IP Address Type: ☒ IPv4 ☐ IPv6

RADIUS IP Address:

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	802.11k	DSCP Priority	VLAN Priority	Security	MAC Auth Type
0	<input checked="" type="checkbox"/>	100	Work Network	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼	None ▼	Disabled ▼
1	<input checked="" type="checkbox"/>	1	Free Network	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼	WPA Enterprise ▼	Disabled ▼

WPAVersions: ☒ WPA-TKIP ☒ WPA2-AES

☐ Enable pre-authentication

☒ Use global RADIUS server settings

RADIUS Domain:

RADIUS IP Address Type: ☒ IPv4 ☐ IPv6

RADIUS IP Address:

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: ▼

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

Session Key Refresh Rate: (Range:30-86400 ,0 Disables)

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 16													
Network	Station	Status		From Station				To Station					
		Authenticated	Associated	Packets	Bytes	Drop Packets	Drop Bytes	TS Violate	Pkts	Packets	Bytes	Drop Packets	Drop
wlan0	58:1f:aa:44:eb:ad	Yes	Yes	111	15140	0	0			102	45093	0	0
wlan0	d0:92:9e:07:57:78	Yes	Yes	138	26734	0	0			110	31065	0	0
wlan0	f4:f5:a5:83:70:fa	Yes	Yes	5448	528168	0	0			15961	22148460	0	0
wlan0	00:1d:07:b1:8c:ee	Yes	Yes	1481	191754	0	0			1046	418497	0	0
wlan0	70:72:0d:bd:da:d9	Yes	Yes	4476	489970	0	0			6605	8331873	0	0
wlan0	40:b0:fa:c7:ca:8e	Yes	Yes	7770	884486	0	0			5007	2161644	0	0
wlan0	9c:3a:af:d5:e9:84	Yes	Yes	32926	2834373	0	0			31354	4383820	0	0
wlan0vap1	94:01:c2:c1:74:89	Yes	Yes	14199	1458838	0	0			22150	29841569	0	0
wlan0vap1	38:0b:40:3f:eb:a2	Yes	Yes	690	103043	0	0			567	279733	0	0
wlan0vap1	90:a4:de:5d:08:32	Yes	Yes	52392	6096071	0	0			36252	9425775	0	0
wlan0vap1	0c:37:dc:d3:96:80	Yes	Yes	19323	2697781	0	0			19262	21625325	0	0
wlan1	c8:6f:1d:60:c1:1e	Yes	Yes	732	115851	0	0			616	196921	0	0
wlan1	40:b3:95:5a:82:f4	Yes	Yes	507	115331	0	0			218	78406	0	0
wlan1	84:38:35:50:20:88	Yes	Yes	76996	7637455	0	0			137346	111082212	0	0
wlan1	8c:29:37:db:14:64	Yes	Yes	997	117292	0	0			834	484022	0	0
wlan1	a4:67:06:71:4f:90	Yes	Yes	16371	10027889	0	0			11946	3689300	0	0

The list of third-party access points in WOP-12ac 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	Rate	Signal	Beacons	Last Beacon	Rates
Grant	00:ac:ac:07:cc:00	wlan0	100	AP	try	On	On	2.4	6	1		110091	Mon Apr 6 15:39:28 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:63:55:e3	wlan0	100	AP	ELTEX-55E2	On	On	2.4	6	1		20	Mon Mar 30 16:04:54 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:5a:bd:e3	wlan0	100	AP	ELTEX-BDE2	On	On	2.4	6	1		10	Tue Mar 24 02:32:34 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	ac:81:12:76:94:04	wlan0	100	AP	ELTEX-2326	On	On	2.4	1	1		28	Wed Apr 1 13:13:09 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:5b:19:53	wlan0	100	AP	ELTEX-1952	On	On	2.4	6	1		4	Mon Mar 23 14:35:39 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:5b:19:8b	wlan0	100	AP	ELTEX-198A	On	On	2.4	1	1		725	Thu Apr 2 09:04:20 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:70:c7:df	wlan0	100	AP	ELTEX-C7DE	On	On	2.4	1	1		1300	Wed Apr 1 11:00:48 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:b0:03:80	wlan0	100	AP	Eltex-Local	On	On	2.4	1	1		44	Mon Apr 6 11:41:01 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:64:5e:df	wlan0	100	AP	ELTEX-5EDE	On	On	2.4	1	1		16	Fri Apr 3 03:49:21 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:64:3a:ff	wlan0	100	AP	ELTEX-3AFE	On	On	2.4	6	1		25	Thu Mar 26 00:40:59 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:64:07:e3	wlan0	100	AP	ELTEX-07E2	On	On	2.4	6	1		12	Thu Mar 26 04:32:36 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	a8:f9:4b:c0:27:a1	wlan0	100	AP	ELTEX-27A0	On	On	2.4	6	1		27	Fri Apr 3 07:34:57 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	20:10:7a:af:69:8a	wlan0	100	AP	ELTEX-AC19	On	On	2.4	11	1		79	Mon Apr 6 11:51:03 2015	1,2,5,5,11,18,24,36,54,6,9,12,48
Grant	20:10:7a:c8:70:86	wlan0	100	AP	ELTEX-7962	On	On	2.4	11	1		27	Mon Apr 6 07:26:21 2015	1,2,5,5,11,18,24,36,54,6,9,12,48

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

View events generated by this access point

Options

Persistence ☒ Enabled ☐ Disabled

Severity

Depth (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 (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
Apr 6 2015 16:22:14	info	cportald[1617]	Captive Portal 90:a4:de:5d:08:32 session is disconnected because of cp authentication timeout.
Apr 6 2015 16:21:38	debug	hostapd[1667]	station: 00:1d:07:b1:8c:ee deauthenticated
Apr 6 2015 16:21:38	info	hostapd[1667]	STA 00:1d:07:b1:8c:ee deauthed from BSSID a8:f9:4b:b0:05:40 reason 4: Disassociated due to inactivity
Apr 6 2015 16:17:14	info	cportald[1617]	Captive Portal 90:a4:de:5d:08:32 session is disconnected because of cp authentication timeout.
Apr 6 2015 16:13:24	debug	hostapd[1667]	station: ec:f3:5b:87:94:8f deauthenticated
Apr 6 2015 16:13:24	info	hostapd[1667]	STA ec:f3:5b:87:94:8f disassociated from BSSID a8:f9:4b:b0:05:41 reason 1: Unspecified Reason
Apr 6 2015 16:13:22	info	hostapd[1667]	STA ec:f3:5b:87:94:8f associated with BSSID a8:f9:4b:b0:05:41
Apr 6 2015 16:13:22	info	hostapd[1667]	Assoc request from ec:f3:5b:87:94:8f BSSID a8:f9:4b:b0:05:41 SSID Eltex-Guest
Apr 6 2015 16:13:18	info	cportald[1617]	Captive Portal 84:38:35:50:20:88 client logged out.
Apr 6 2015 16:12:13	info	cportald[1617]	Captive Portal 90:a4:de:5d:08:32 session is disconnected because of cp authentication timeout.
Apr 6 2015 16:11:55	info	hostapd[1667]	STA 58:1f:aa:44:ab:ad associated with BSSID a8:f9:4b:b0:05:40
Apr 6 2015 16:11:55	info	hostapd[1667]	Assoc request from 58:1f:aa:44:ab:ad BSSID a8:f9:4b:b0:05:40 SSID Eltex-Local
Apr 6 2015 16:11:55	err	hostapd[1667]	trying to deauthenticate to station 58:1f:aa:44:ab:ad, but not authenticated
Apr 6 2015 16:11:55	err	hostapd[1667]	trying to update accounting statistics, station 58:1f:aa:44:ab:ad not found

To obtain more detailed information, read the full user manual ([WOP-12ac. 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-12ac 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-12ac becomes a master of the cluster. If the devices belonging to the cluster are found, WOP-12ac 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-12ac 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.

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

Manage access points in the cluster

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

Softwlc mode only for Captive Portal Instance Configuration

Clustering:

Clustering Options...

Enter the location of this AP.

Location:

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

Cluster Name:

Clustering IP Version: ☐ IPv6 ☒ IPv4

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

Click "Update" to save the new settings.

Single IP Management...

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

Click "Update" to save the new settings.

Secure Join Clustering...

Secure Mode: ☐ Enabled ☒ Disabled

Pass Phrase: (8 - 63 characters)

Reauthentication Timeout: (Sec, Range: 300 - 86400)

Click "Update" to save the new settings.

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.

Manage access points in the cluster

Access Points...

Clustering:

Location	MAC Address	IP Address	Cluster-Priority	Cluster-Controller
not set	A8:F9:4B:B0:B5:40	192.168.15.64	-1	no

Clustering Options...

Location:

Cluster Name:

Clustering IP Version: ☐ IPv6 ☒ IPv4

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

Click "Update" to save the new settings.

Single IP Management...

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

Click "Update" to save the new settings.

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 ...

automatically re-assigning channels

Current Channel Assignments

IP Address	Radio	Band	Channel	Status
192.168.15.64	A8:F9:4B:B0:B5:50	A	52	up
192.168.15.64	A8:F9:4B:B0:B5:40	B/G	11	up

Advanced

Change channels if interference is reduced by at least (Range: 1...100)

Refresh when access point is added to the cluster (Range: enable/disable)

Determine if there is better set of channel settings every (Range: 1 Day...1 Week)

Click "Update" to save the new settings.

Transmit Power Control ...

automatically re-assigning tx power

RSSI threshold 2.4 GHz (Range: -100...-30)

RSSI threshold 5 GHz (Range: -100...-30)

Interval (Range: 1800...86400 or 0)

Advanced

Minimal Tx Power (Range: 6...30)

Active Scan Mode ☒

Debug Mode ☐

Monitoring

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

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.

9.4 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:

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 selecting 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** – 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.

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		
ttt555555555555	49			
Default	61			
Default	52		46	
tester2			45	
tester7			49	
tester6			40	
tester12			41	

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.

9.5 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:

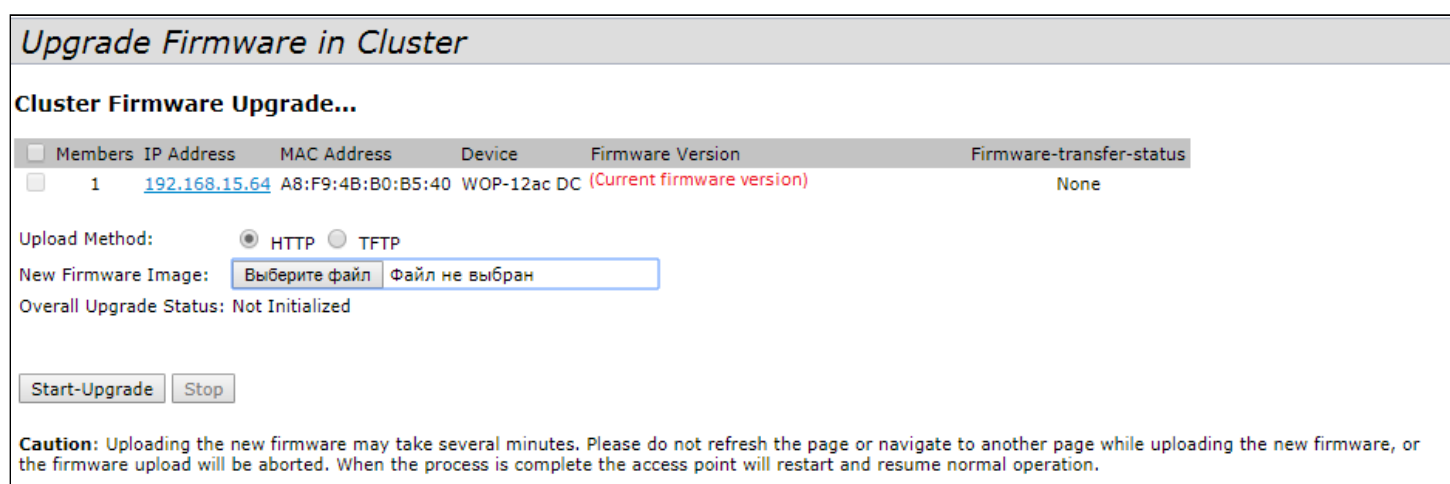
- through web interface;
- through DHCP Autoprovisioning (opt 66, opt 67).

9.5.1 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:



Upgrade Firmware in Cluster

Cluster Firmware Upgrade...

Members	IP Address	MAC Address	Device	Firmware Version	Firmware-transfer-status	
<input type="checkbox"/>	1	192.168.15.64	A8:F9:4B:B0:B5:40	WOP-12ac DC	(Current firmware version)	None

Upload Method: ☒ HTTP ☐ TFTP

New Firmware Image:

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.

- **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. «*Wop12ac-1.8.0.636.tar*» is used in the example;
- **Server IP** – enter an IP address of TFTP server on which firmware file is saved. «*192.168.15.250*» 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.

9.5.2 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. a) Place the "**wop12.manifest**" file on TFTP server, the file should contain the following string:

VERSION= "1.20.0.X" WOP-12ac-1.20.0.X.tar.gz,

where

WOP-12ac-1.20.0.X.tar.gz – name of the archive containing firmware for WEP-12ac;

1.20.0.X – a firmware version included to the archive.

The firmware version might be viewed in «version» file in firmware archive.

1. b) Place archive with firmware for WOP-12ac on TFTP server.
2. c) Correct DHCP server settings (dhcpd.conf) as follows:

```
option tftp-server-name "192.168.10.1";
```

```
option bootfile-name "wop12.manifest";
```

where

192.168.10.1 – TFTP server address;

wop12.manifest – 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/>