v1.14_Using TLS certificates for user authorization

Generating a server certificate

Server certificate can be generated when the package `eltex-radius-nbi` is installed. Specify certificate parameters during the package installation.

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-radius-nbi
...

Do you want to generate server certificate? [y/N]: y

 - Enter pass:
 - Repeat pass:
 - Enter period (in days): 365
 - Enter country [RU]:
 - Enter state [Novosibirsk Oblast]:
 - Enter locatity [Novosibirsk]:
 - Enter organization [Eltex]:
 - Enter organization unit [Wireless network IT]:
 - Enter email [eltex@eltex.nsk.ru]:
```

If you already have `eltex-radius-nbi`, it should be reinstalled.

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get remove eltex-radius-nbi

root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-radius-nbi
```

After that, a certificate will be generated.

```
Successfully generated the server certificate
URL of the server certificates:
   http://localhost:8080/eltex-radius-nbi/certificates/server.zip
Run the script to setup Eltex RADIUS server:
   /var/lib/eltex-radius-nbi/setup_er_eap.sh

 - Reconfigure file '/etc/eltex-radius-nbi/radius_nbi_config.txt'

SoftWLC Northbound is installed. Tomcat service will be restarted...
To check the service works, open the URL:
   http://localhost:8080/axis2/services/RadiusNbiService?wsdl
To read documentation, visit the following URL:
   http://localhost:8080/eltex-radius-nbi/asciidoc/
```

Then run the script **setup_er_eap.sh**:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# cd /var/lib/eltex-radius-nbi/
root@vagrant-ubuntu-trusty-64:./setup_er_eap.sh
eltex-radius stop/waiting
eltex-radius start/running, process 2317
```

Creating a TLS certificate at users

A created server certificate allows generating certificated for Enterprise users. If a TLS certificate should be used for authorization, it must be specified during Enterprise user creation.

Step-by-step description of certificate creation process:

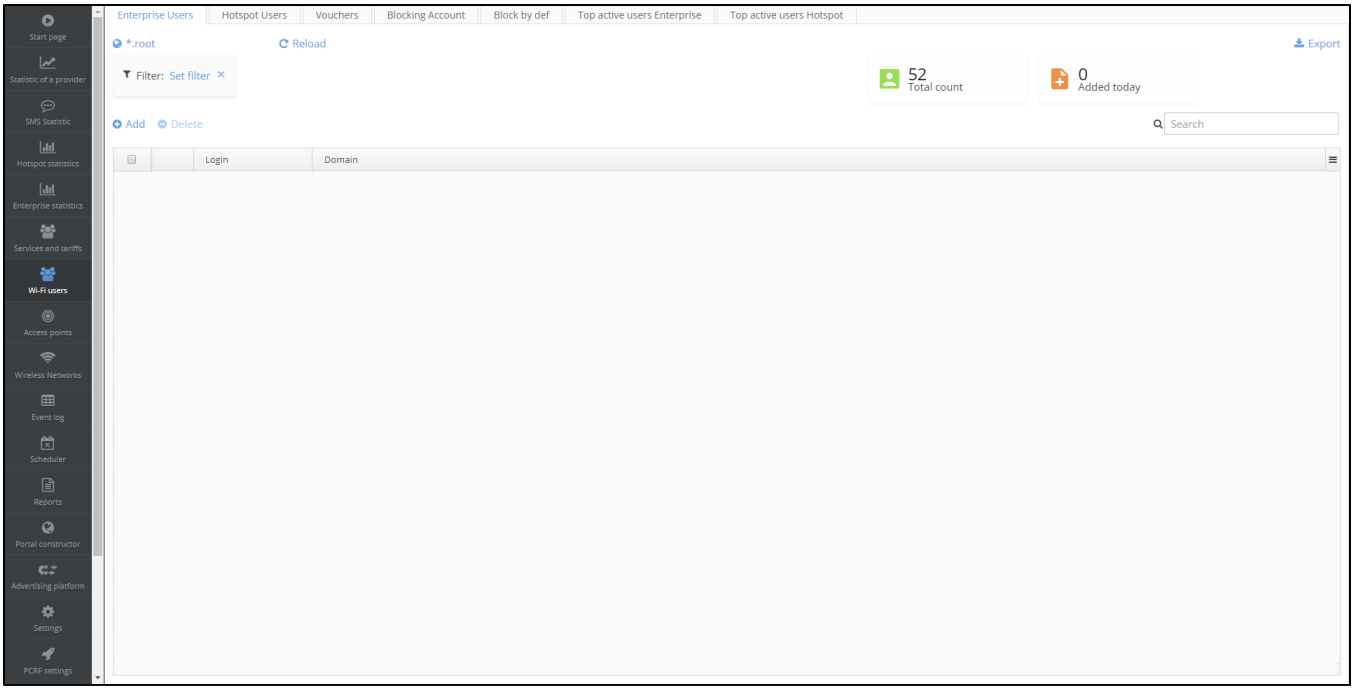
1. Open the file **cat /etc/eltex-radius-nbi/radius_nbi_config.txt** and specify an address that is referred by a user to request the Admin Panel (127.0.0.1 by default).

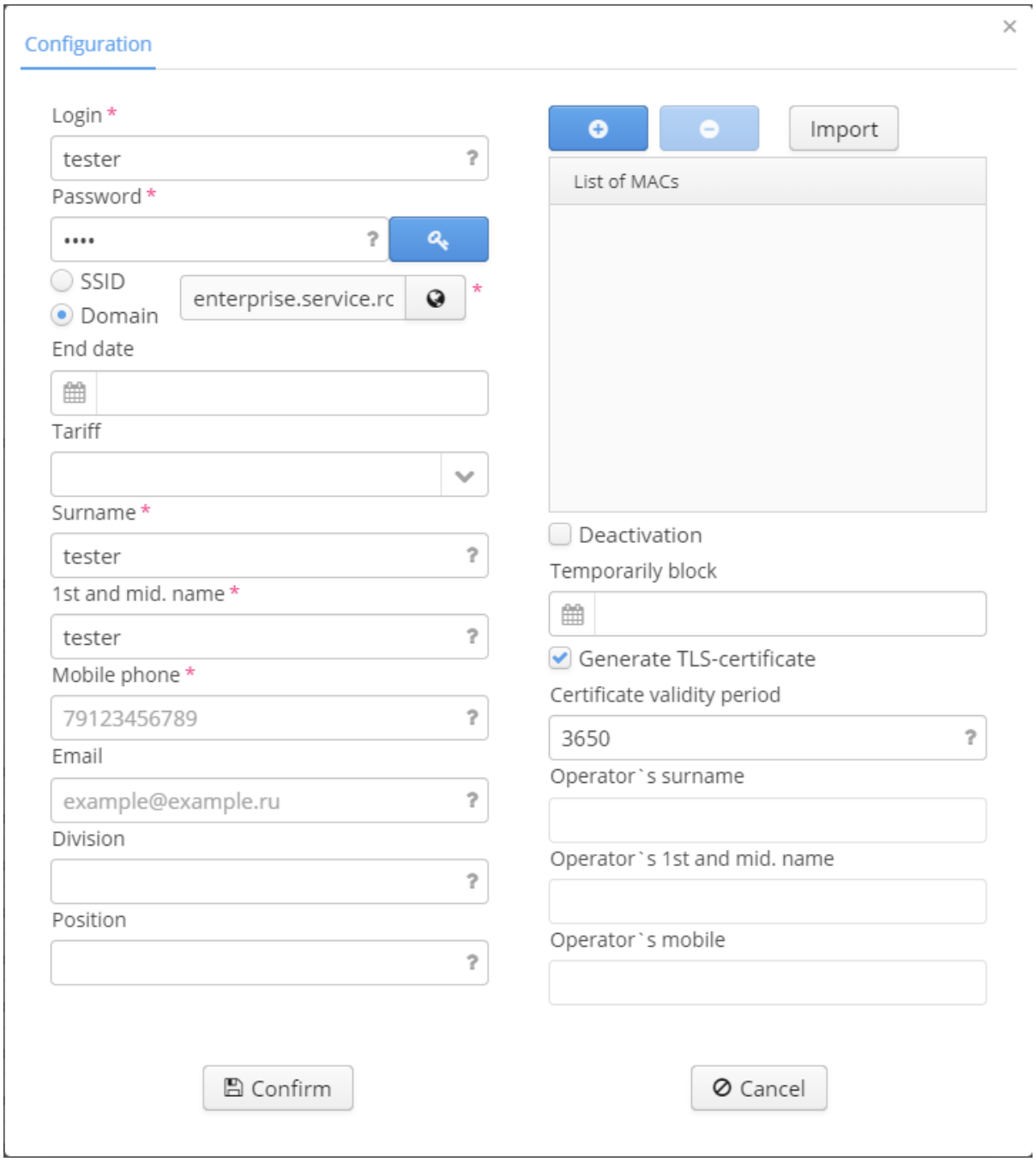
```
# tomcat url

tomcat.host=127.0.0.1

tomcat.port=8080
```

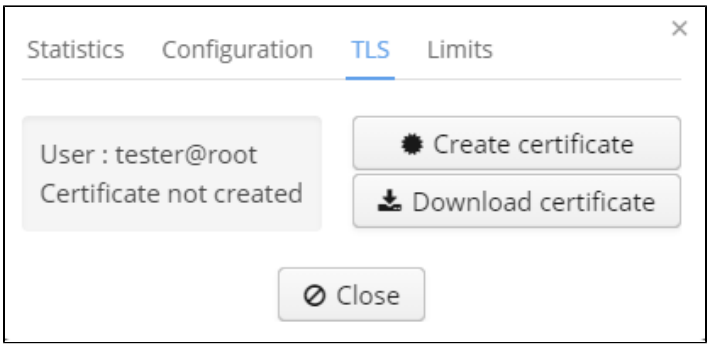
2. Enter the Admin Panel and open the tab "Wi-Fi Users" -> "Enterprise users". Click "Add".





3. Specify user parameters and click the checkbox "Create certificate".

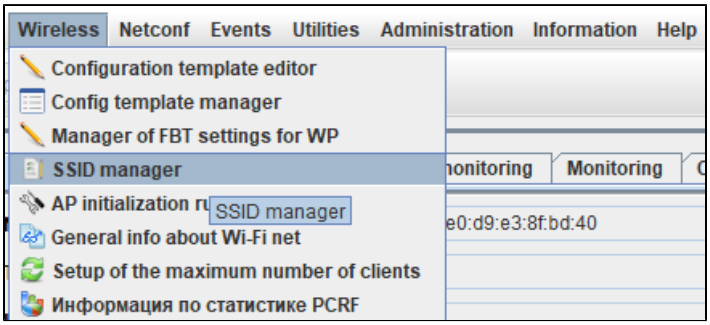
By default, a certificate is valid for 3650 days. Change this parameter if necessary.

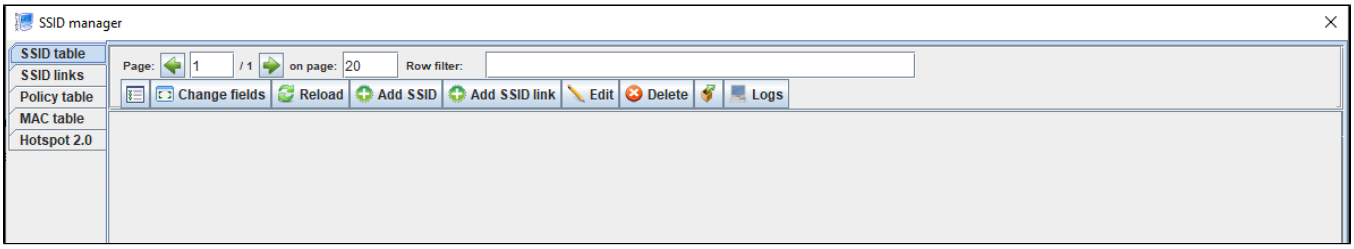


After a user is created, his parameters can be seen. Check the tab "TLS" to verify a certificate has been generated.

Creating an Enterprise SSID with support for TLS

Open the SSID manager in the *"Wireless"* menu.





Click *"Add SSID"*.

Specify the following key parameters:

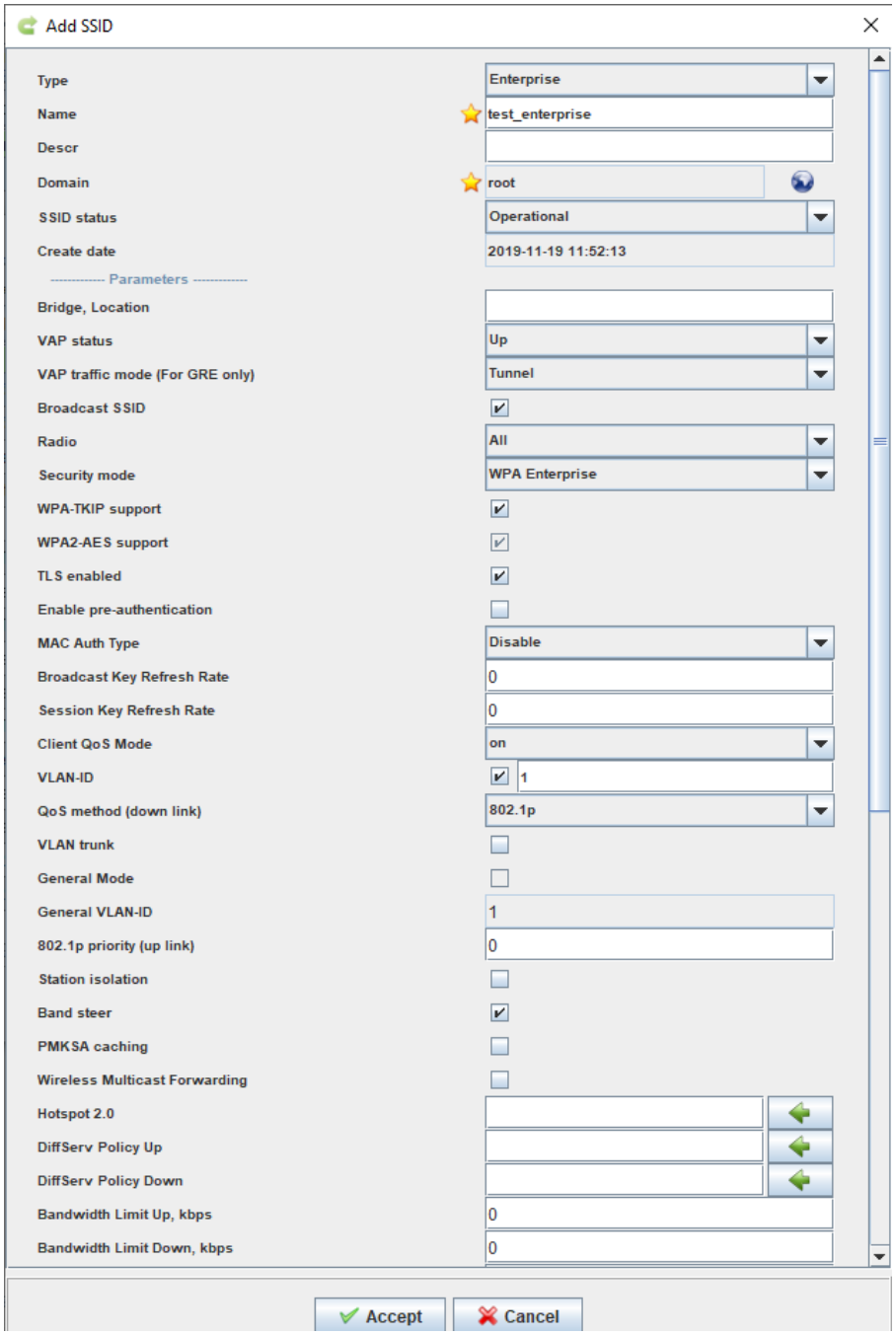
```
Type - Enterprise
Name - test_enterprise
Domain - root
Security mode - WPA Enterprise
RADIUS IP Address - 192.168.50.1 (ip address of your Radius server).
RADIUS Key - eltex
RADIUS accounting - up
RADIUS accounting period - 600
```

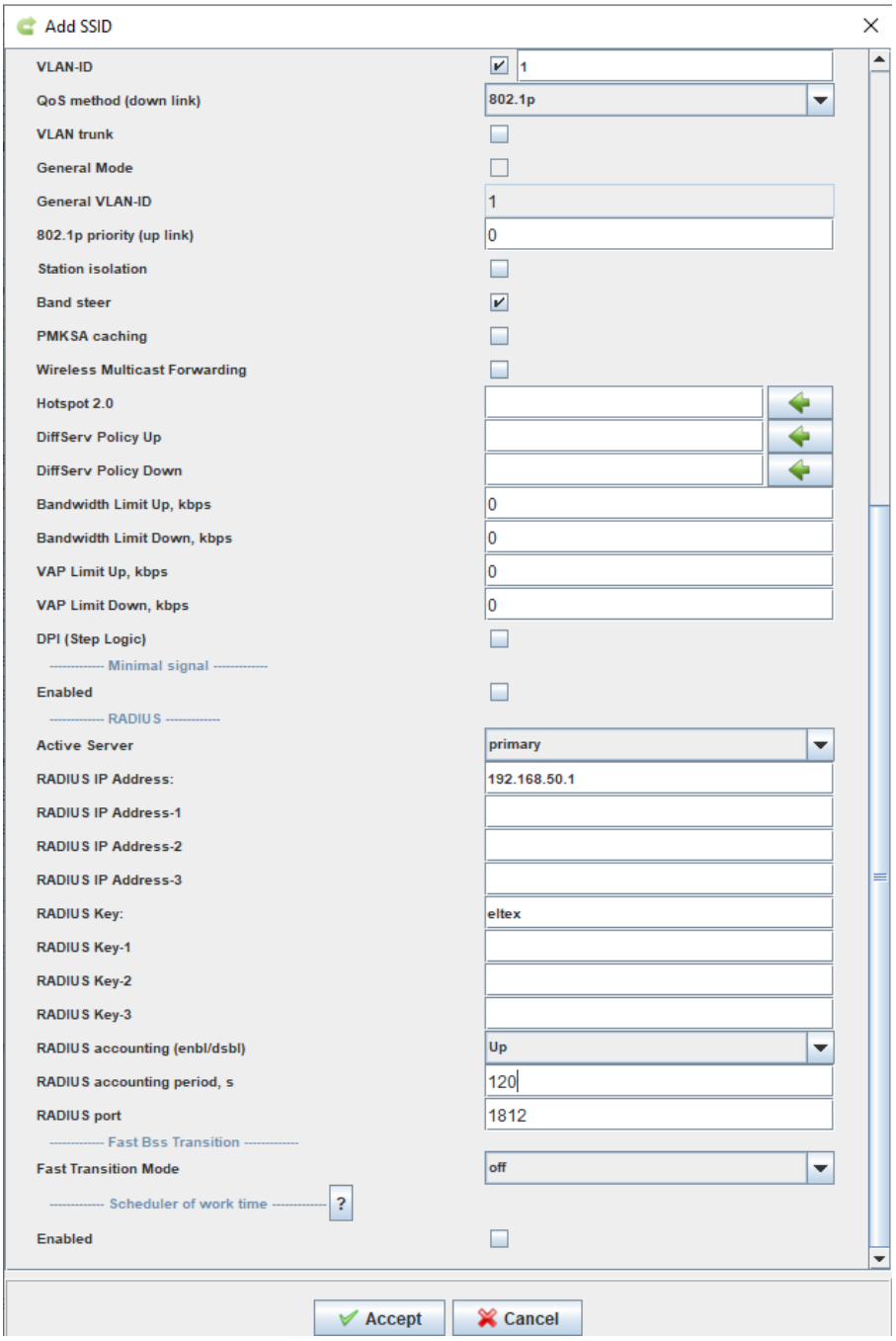
Select radio interfaces to which a created SSID will be assigned.

When a SSID is assigned to all radio interfaces *("Radio" - "All")*, it is recommended to enable *"Bandsteer"* (click the checkbox) for priority connection of devices supporting the both ranges to the 5 GHz network.

When a SSID is assigned to one radio interface, the mode *"Bandsteer"* should be disabled.

Click the checkbox *"TLS enabled"*.

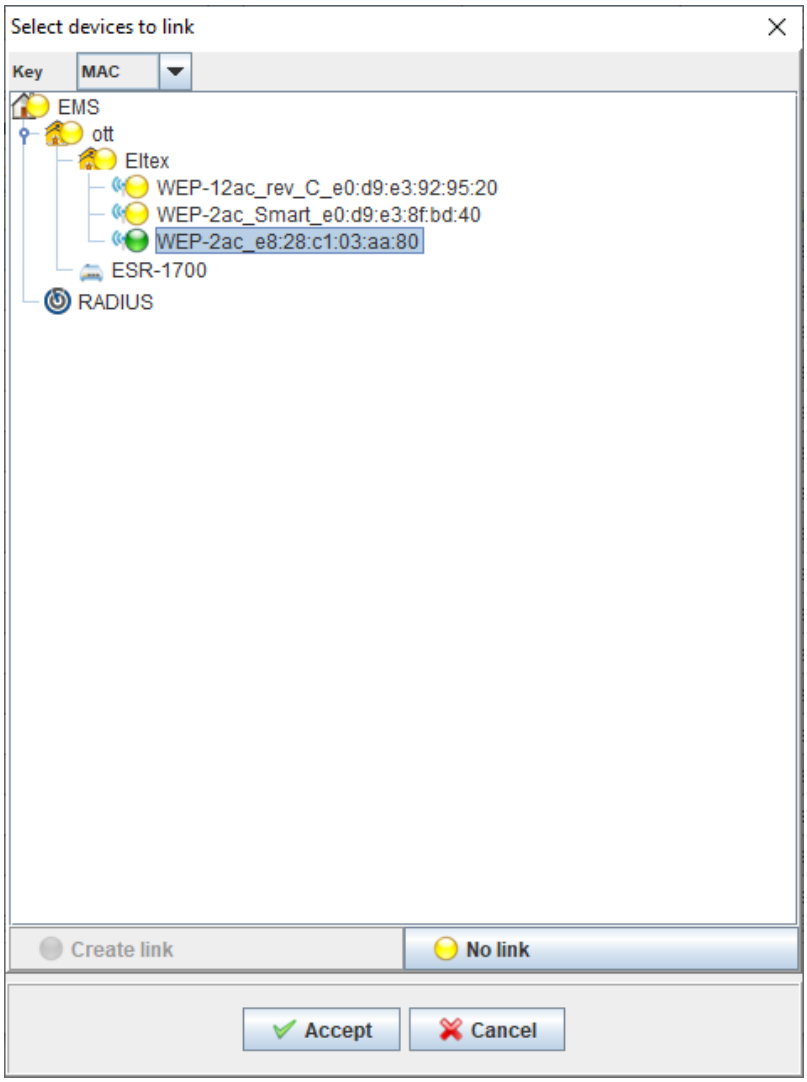

Add SSID
Type
Enterprise
Name
test_enterprise
Descr
Domain
root
SSID status
Operational
Create date
2019-11-19 11:52:13
---------- Parameters ----------
Bridge, Location
VAP status
Up
VAP traffic mode (For GRE only)
Tunnel
Broadcast SSID
Radio
All
Security mode
WPA Enterprise
WPA-TKIP support
WPA2-AES support
TLS enabled
Enable pre-authentication
MAC Auth Type
Disable
Broadcast Key Refresh Rate
0
Session Key Refresh Rate
0
Client QoS Mode
on
VLAN-ID
1
QoS method (down link)
802.1p
VLAN trunk
General Mode
General VLAN-ID
1
802.1p priority (up link)
0
Station isolation
Band steer
PMKSA caching
Wireless Multicast Forwarding
Hotspot 2.0
DiffServ Policy Up
DiffServ Policy Down
Bandwidth Limit Up, kbps
0
Bandwidth Limit Down, kbps
0
Accept
Cancel



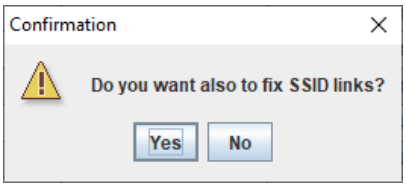
After the button *"Accept"* is clicked, a created SSID will be displayed in *"SSID table"*.

Assign a SSID to access points by selecting a created SSID and clicking *"Add SSID link"*.

Select a key for linking in the appeared window. It can be a MAC address or a node's domain. Select devices to link (access points or nodes) and click *"rea te a link"*, the corresponding indicator will turn from yellow to green. Click *"Accept"*.



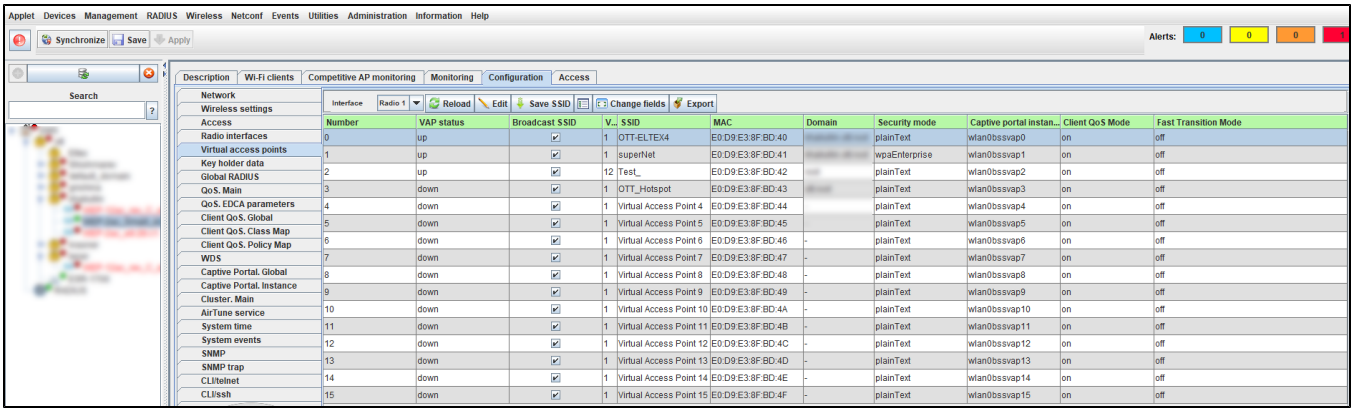
A window with the question "Do you want also to fix SSID links?" will be opened. If it is necessary to assign a created SSID to access points immediately, click "Yes". If a link should be added to the table, but should not be applied to an access point, click "No". If necessary, a SSID can be assigned to an access point by clicking "Repair" on the tab "SSID links". Otherwise, a link will be fixed by a corresponding monitor (once a day by default).



A SSID assigning process can be managed via the tab *"Operations log".*

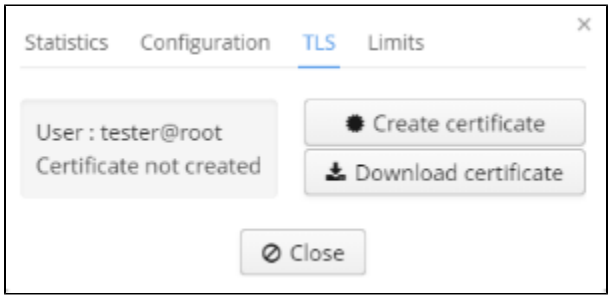
A created link will be displayed on the tab *"SSID links".*

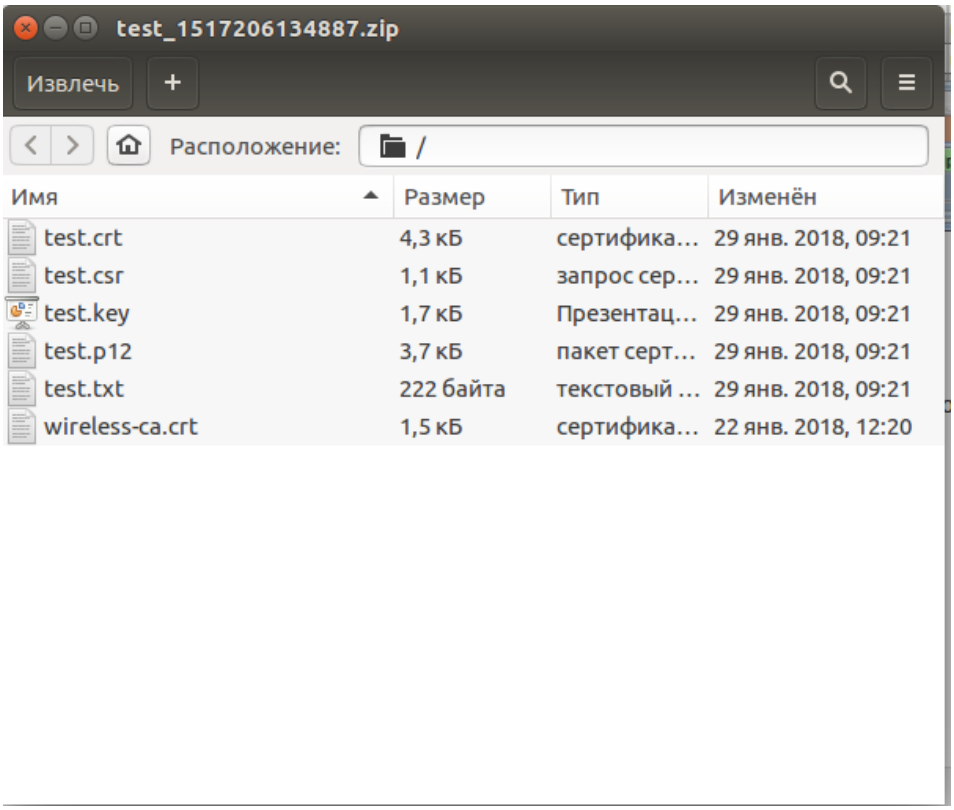
A SSID will be assigned to the first A result can be seen on the tab *"Configuration/Virtual access points".*



Installing a certificate to a client's device

It is necessary to install a certificate to a client's device. To do that, enter the Admin Panel, go to the section "Wi-Fi users/Enterprise users" and select a user created earlier. In the opened window and click the button "Create certificate" on the tab "TLS".





The .txt file contains necessary information on a certificate. The parameters Name and Password will be necessary.

Name: test
Domain: root
Password: test
Period: 3650
Organization name: Eltex
Country code: RU
State: Novosibirsk Oblast
Locality: Novosibirsk
Organization unit name: Wireless network IT
Contact e-mail: eltex@eltex.nsk.ru

> The value "test" of the "Name" parameter matches the name of the user created via the Admin panel. The value of "Password" is the same.

Contents of the downloaded archive should be copied to a client's device.