

# v1.14\_Using TLS certificates for user authorization

- [Generating a server certificate](#)
- [Creating a TLS certificate at users](#)
- [Creating an Enterprise SSID with support for TLS](#)
- [Installing a certificate to a client's device](#)

## 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:/var/lib/eltex-radius-nbi# ./setup_er_eap.sh
eltex-radius stop/waiting
eltex-radius start/running, process 2317
```

## Creating a TLS certificate at users

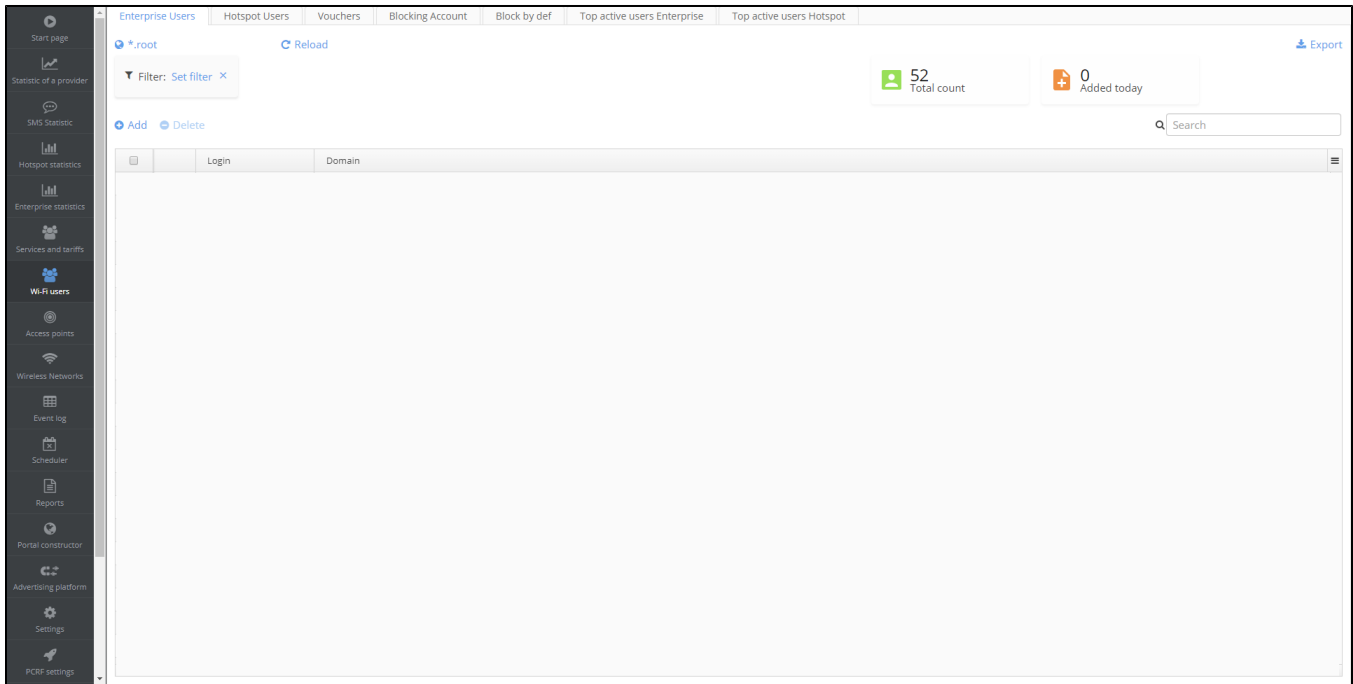
A created server certificate allows generating certificated for Enterprise users. If a TLS certificate should be used for authorization, it must be specified during Enterprise user creation.

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".



Configuration

×

Login \*

tester?

Password \*

....? 🔑

☐ SSID
 

enterprise.service.rc \*

☒ Domain

End date

📅

Tariff

Surname \*

tester?

1st and mid. name \*

tester?

Mobile phone \*

79123456789?

Email

example@example.ru?

Division

Position

+

-

Import

List of MACs

☐ Deactivation
 

Temporarily block

📅

☒ Generate TLS-certificate
 

Certificate validity period

3650?

Operator`s surname

Operator`s 1st and mid. name

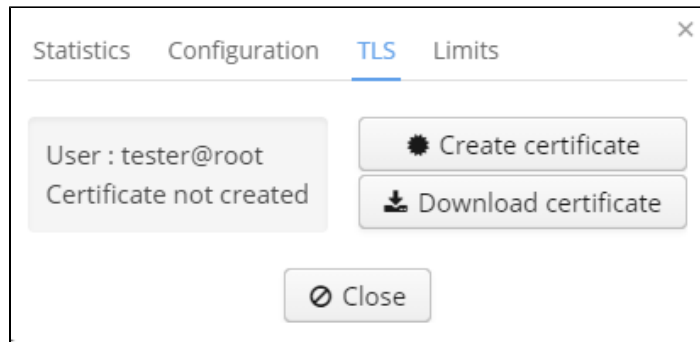
Operator`s mobile

📁 Confirm

⌛ Cancel

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

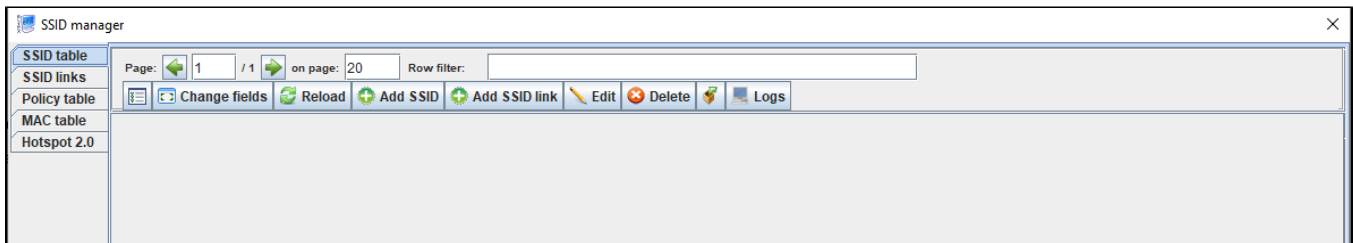
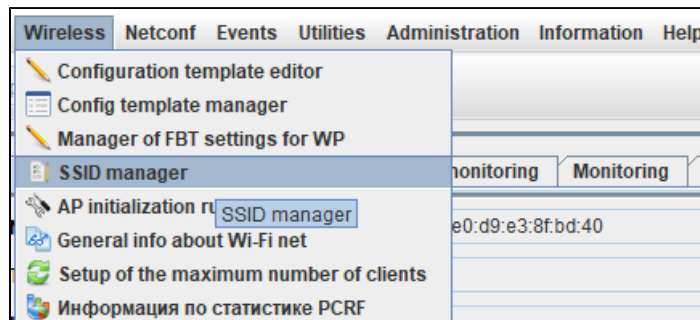
By default, a certificate is valid for 3650 days. Change this parameter if necessary.



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

☒

TL S 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

Add SSID

☒

VLAN-ID

1

802.1p

QoS method (down link)

☐

VLAN trunk

☐

General Mode

1

General VLAN-ID

0

802.1p priority (up link)

☐

Station isolation

☒

Band steer

☐

PMKSA caching

☐

Wireless Multicast Forwarding

Hotspot 2.0

DiffServ Policy Up

DiffServ Policy Down

0

Bandwidth Limit Up, kbps

0

Bandwidth Limit Down, kbps

0

VAP Limit Up, kbps

0

VAP Limit Down, kbps

☐

DPI (Step Logic)

Minimal signal

☐

Enabled

RADIUS

primary

Active Server

192.168.50.1

RADIUS IP Address:

RADIUS IP Address-1

RADIUS IP Address-2

RADIUS IP Address-3

eltex

RADIUS Key:

RADIUS Key-1

RADIUS Key-2

RADIUS Key-3

Up

RADIUS accounting (enbl/dsbl)

120

RADIUS accounting period, s

1812

RADIUS port

Fast Bss Transition

off

Fast Transition Mode

Scheduler of work time

☐

Enabled

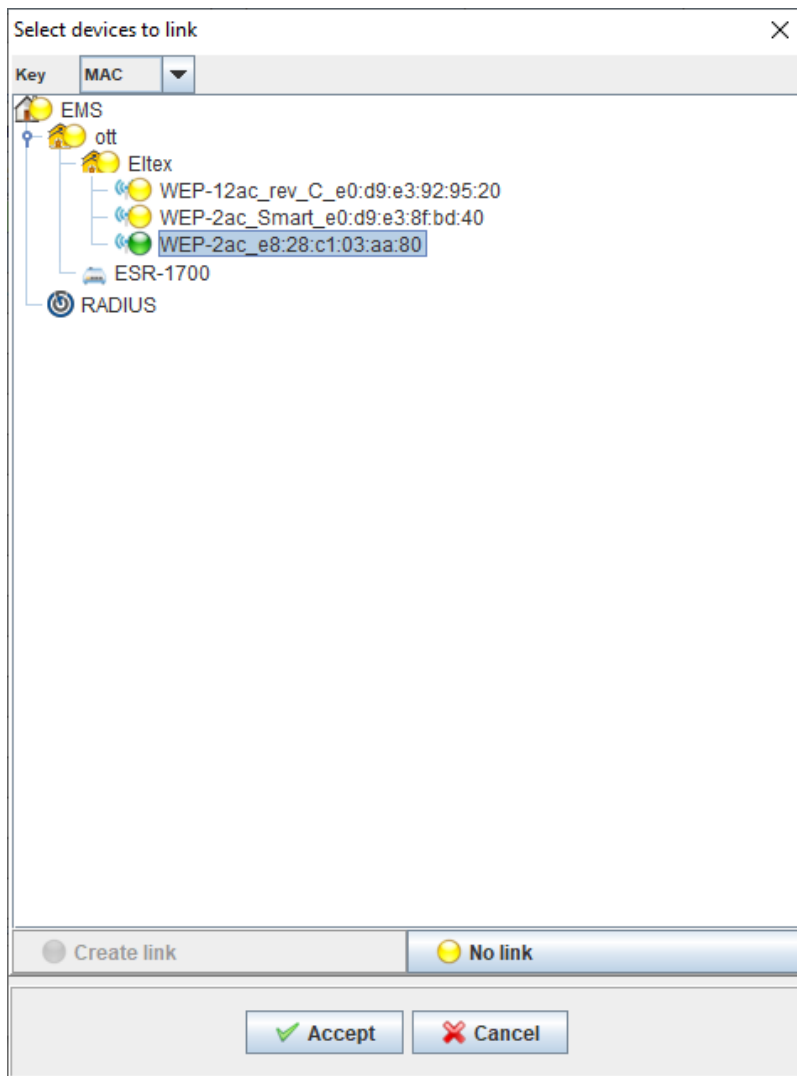
Accept

Cancel

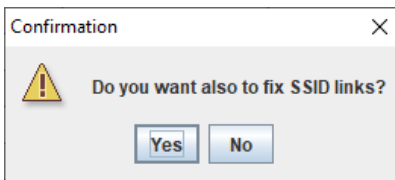
After the button "Accept" is clicked, a created SSID will be displayed in "SSID table".

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 "reate 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".

Applet	Devices	Management	RADIUS	Wireless	Netconf	Events	Utilities	Administration	Information	Help
Synchronize Save Apply Alerts: 5 0 0 1										
Description Wi-Fi clients Competitive AP monitoring Monitoring Configuration Access										
Network										
Wireless settings										
Access										
Radio interfaces										
Key holder data										
Global RADIUS										
QoS, Main										
QoS, EDC parameters										
Client QoS, Global										
Client QoS, Class Map										
Client QoS, Policy Map										
WDS										
Captive Portal, Global										
Captive Portal, Instance										
Cluster, Main										
AirTune service										
System time										
System events										
SNMP										
SNMP trap										
CLI/Net										
CLI/ssh										
Interface Radio 1 Reload Edit Save SSID Change fields Export										
Number VAP status Broadcast SSID V. SSID MAC Domain Security mode Captive portal instan... Client QoS Mode Fast Transition Mode										
0 up 1 OTT-ELTEX4 E0:D9:E3:8F:BD:40 - plainText wlan0bssvap0 on off										
1 up 1 superNet E0:D9:E3:8F:BD:41 - wpaEnterprise wlan0bssvap1 on off										
2 up 12 TestL E0:D9:E3:8F:BD:42 - plainText wlan0bssvap2 on off										
3 down 1 OTT_Hotspot E0:D9:E3:8F:BD:43 - plainText wlan0bssvap3 on off										
4 down 1 Virtual Access Point 4 E0:D9:E3:8F:BD:44 - plainText wlan0bssvap4 on off										
5 down 1 Virtual Access Point 5 E0:D9:E3:8F:BD:45 - plainText wlan0bssvap5 on off										
6 down 1 Virtual Access Point 6 E0:D9:E3:8F:BD:46 - plainText wlan0bssvap6 on off										
7 down 1 Virtual Access Point 7 E0:D9:E3:8F:BD:47 - plainText wlan0bssvap7 on off										
8 down 1 Virtual Access Point 8 E0:D9:E3:8F:BD:48 - plainText wlan0bssvap8 on off										
9 down 1 Virtual Access Point 9 E0:D9:E3:8F:BD:49 - plainText wlan0bssvap9 on off										
10 down 1 Virtual Access Point 10 E0:D9:E3:8F:BD:4A - plainText wlan0bssvap10 on off										
11 down 1 Virtual Access Point 11 E0:D9:E3:8F:BD:4B - plainText wlan0bssvap11 on off										
12 down 1 Virtual Access Point 12 E0:D9:E3:8F:BD:4C - plainText wlan0bssvap12 on off										
13 down 1 Virtual Access Point 13 E0:D9:E3:8F:BD:4D - plainText wlan0bssvap13 on off										
14 down 1 Virtual Access Point 14 E0:D9:E3:8F:BD:4E - plainText wlan0bssvap14 on off										
15 down 1 Virtual Access Point 15 E0:D9:E3:8F:BD:4F - plainText wlan0bssvap15 on off										

## Installing a certificate to a client's device

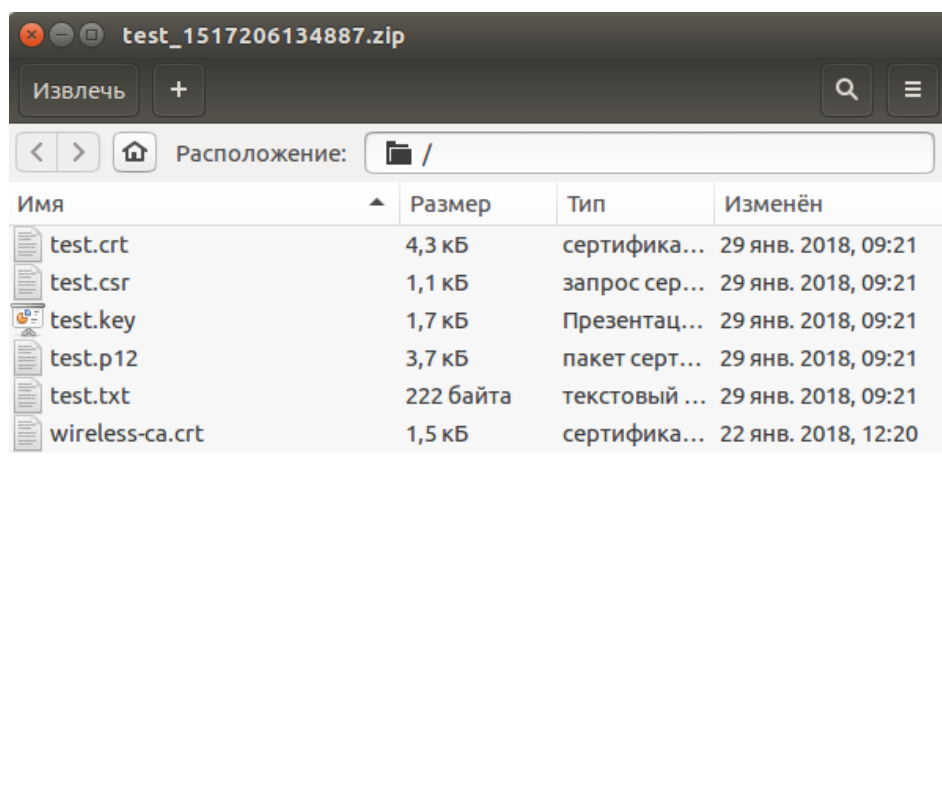
It is necessary to install a certificate to a client's device. To do that, enter the Admin Panel, go to the section "Wi-Fi users/Enterprise users" and select a user created earlier. In the opened window and click the button "Create certificate" on the tab "TLS".

Statistics Configuration TLS Limits

User : tester@root  
Certificate not created

Create certificate  
Download certificate

Close



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](mailto: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.