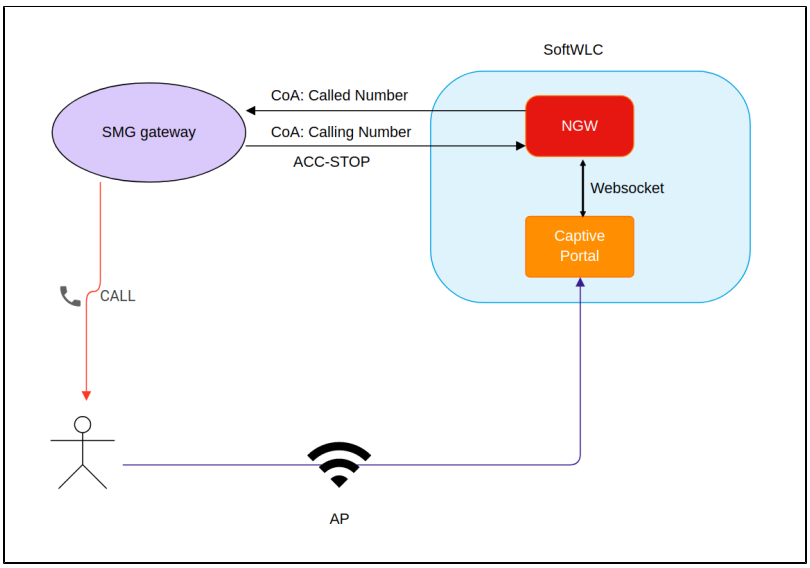
v1.14_Configuring call back authorization

Interaction scheme



Connection steps:

- A user selects call back authorization when connecting to the Captive Portal and enters a phone number;
- Eltex-portal sends information on a Called number to the service eltex-ngw via Websocket;
- Eltex-ngw transfers information on a Called number to an SMG gateway via a CoA request;
- SMG gateway makes a call from a number keeped in a number pool and sends this number (Calling number) to a user in CoA-ACK;
- After a user takes a call (which is dropped then), rejects or ignores it, the SMG gateway will send an ACC-STOP RADIUS packet with confirmation of call receipt to the NGW service;
- A user enters last four digits of the Calling number;
- Authorization has been successfully completed.

For call back authorization to work correctly, provide network connectivity between eltex-ngw and the SMG gateway. A default outgoing port for the service eltex-ngw is UDP/3799, and a port for incoming connections is UDP/1814.

Description

To authorize on the portal, a user should connect to SSID with portal authorization, enter the telephone number and click "Confirm with incoming call". After that, a message "Enter the last 4 digits of the Calling number" will be displayed, and the number will be called.

- It is possible to pick up the phone, then the call will be dropped
- Reject the call
- Await completion of the call

Fill in the field with the last 4 digits of a calling number and click "Enter".
Authorization is completed, the user account will be confirmed.

An interaction scheme is available on Interaction scheme for call back authorization.

Configuring call back authorization

To confirm a user account using a call back, configure eltex-ngw and select "Call to user" as a confirmation method in the portal common settings.
1) eltex-ngw settings for interaction with SMG gateways can be found on Configuring incoming call authorization.
2) Open the Portal Constructor, select a portal on which a confirmation method "Call to user" is selected and go to Common settings. In the section "Confirmation methods" place a check in the checkbox "Call to user". After selecting the checkbox, the field "Call waiting timeout" will be available. A default timeout is 30 seconds.
"Call waiting timeout" is a time period on exceeding of which an input field on the page where the last four digits of a calling number should be entered will become unavailable, and a message *"Unable to make a call. Please, try again."* will be displayed if the acct-stop RADIUS packet from the SMG gateway is not received by Eltex-NGW.

> If a portal user waits when the call ends using callback authorization, the standard "Call waiting timeout" may not be enough. In this case, set the value higher than the call answer waiting timeout (is specified on SMG gateway).

Troubleshooting

1)
"Request execution error" occurs after clicking the button "Confirm with incoming call". Check network connection"

- No connection between Eltex-NGW ang SMG gateway

- Make sure that the address of SMG gateway is specified correctly in the configuration file.

- Make sure that SMG gateway port 3799 is available from the server where Eltex-NGW is locate

```
root@vagrant-ubuntu16-xenial-64-SWLC:~# nmap -sU -p 3799 192.168.114.163

Starting Nmap 7.01 ( https://nmap.org ) at 2019-03-14 09:32 +07
Nmap scan report for 192.168.114.163
Host is up (0.00056s latency).
PORT     STATE         SERVICE
3799/udp open|filtered radius-dynauth
```

- smg.secret specified in the Eltex-NGW configuration file is incorrect

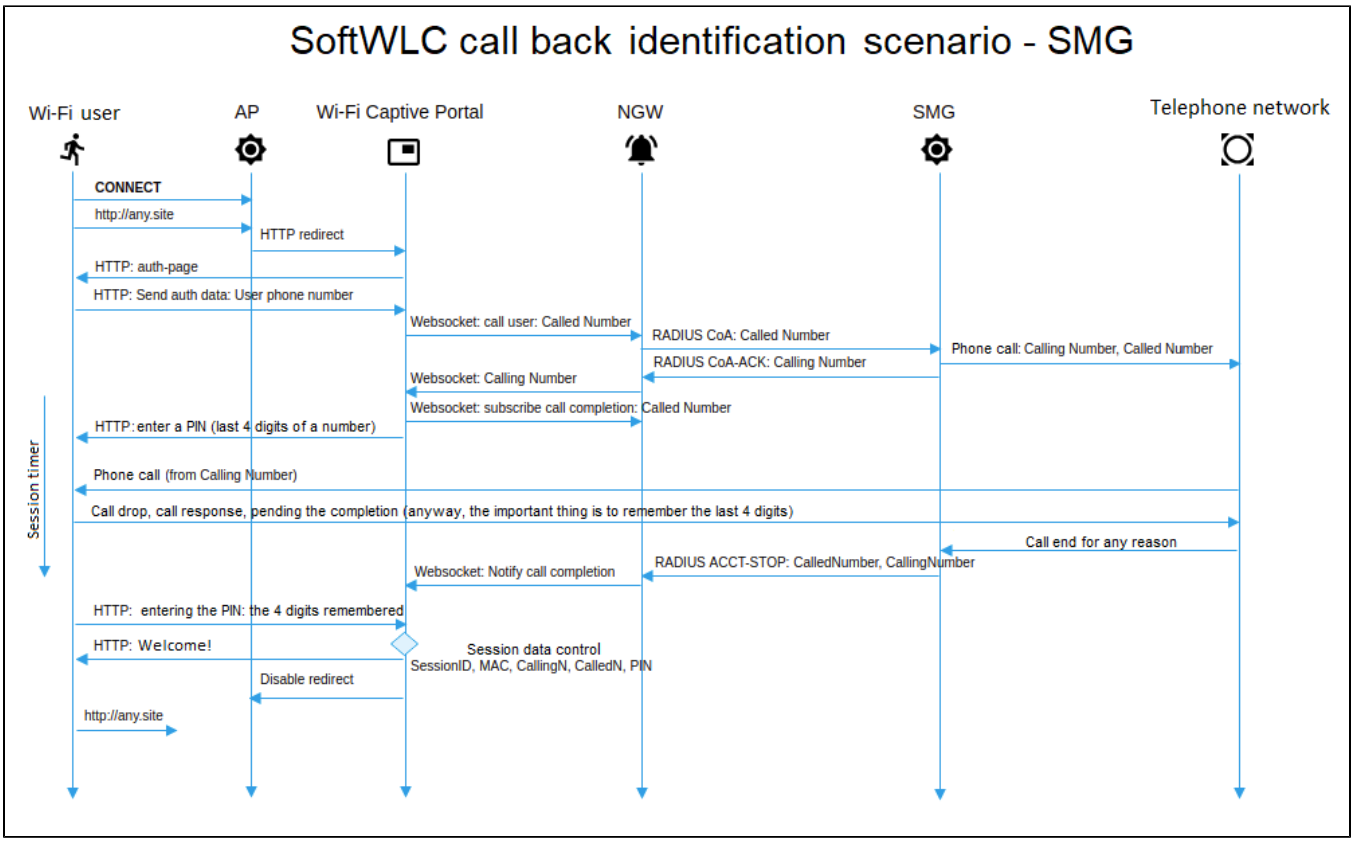
-Make sure that the keys specified for eltex-ngw and for SMG gateway are equal by checking them in the section "RADIUS Authorization servers". If the keys do not match, the gateway will not respond the CoA requests from eltex-ngw.

2)
If a message *"Unable to make a call. Please, try again"* is displayed, the input field is unavailable, but a call was taken.

- Make sure that the port specified in eltex-ngw configuration file is open and available.
- Make sure that the port specified in eltex-ngw configuration file is open and available from SMG gateway (1814 by default).
- The key listen.secret matches the SMG gateway in the section RADIUS Accounting Servers. If the key is incorrect, the following messages will appear in ngw logs:

```
2019-03-14 10:03:06.006 ERROR  SmgGate$Receiver:161 - Incorrect authenticator for incoming radius packet
2019-03-14 10:03:06.006 DEBUG  SmgGate$Receiver:179 - Packet received
2019-03-14 10:03:06.006 ERROR  SmgGate$Receiver:161 - Incorrect authenticator for incoming radius packet
2019-03-14 10:03:07.007 DEBUG  SmgGate$Receiver:179 - Packet received
2019-03-14 10:03:07.007 ERROR  SmgGate$Receiver:161 - Incorrect authenticator for incoming radius packet
```

Identification scenario



SMG configuration

Input data
SMG gateway is configured to interact with PSTN (interfaces for PSTN connection and a dial plan are set) and can make calls. The gateway is configured according to its operation manual.
Requirements to data transmission network configuration
SMG accepts RADIUS Change-of-Authorization (CoA) requests via UDP port **3799**. The network should provide passing of Eltex NGW requests to a specified SMG port.
SMG sends RADIUS Accounting requests to UDP port**1813**. The network should provide passing of SMG requests to a specified Eltex NGW port.
Description of the work
The procedure is initiated via RADIUS Change-of-Authorization (CoA) request (described in RFC 5176). Is used for call back authorization of connection to public networks. A user connects to a network and gets to a WEB portal where an access password is requested and then a user is suggested to enter a password for authorization. After entering a phone number, a user receives a call to this number. A calling number or its part displayed on the user's phone serves as an access password to a public network and should be entered on the WEB portal. To initiate a call, the WEB portal should send a CoA-Request packet with the attribute Called-Station-Id containing user phone number to SMG via RADIUS protocol. CoA-Request example:

```
RADIUS Protocol
Code: CoA-Request (43)
Packet identifier: 0xa0 (160)
Length: 33
Authenticator: ac02dd52e3435a2fa46ed7cd2f7f177d
Attribute Value Pairs
AVP: l=13 t=Called-Station-Id(30): 70123456789
Type: 30
Length: 13
Called-Station-Id: 70123456789
```

If a number can be called, SMG selects a caller's number from a specified number pool and sends it in the attribute Calling-Station-Id of CoA-ACK. After that, SMG initiates a call from the selected number to the user number. Regardless of the result of a call (call drop, user's response or call end on no response timeout), SMG sends information on the call in RADIUS Accounting requests. When a user answers, a call will be dropped. CoA-ACK response example:

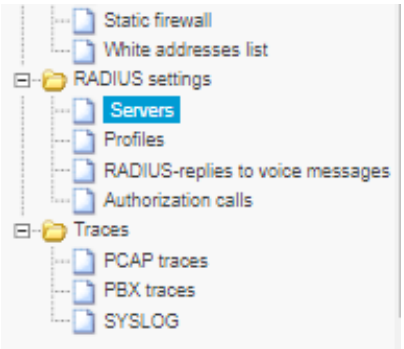
```
RADIUS Protocol
 Code: CoA-ACK (44)
 Packet identifier: 0xa0 (160)
 Length: 33
 Authenticator: 60363e5d4f742df10316cc05b81a42f6
 Attribute Value Pairs
 AVP: l=13 t=Calling-Station-Id(31): 73830019698
 Type: 31
 Length: 13
 Calling-Station-Id: 73830019698
```

If a number specified by a user cannot be called, SMG will respond with a CoA-NAK message without any attributes and will not initiate a call. If a CoA Request was sent from a RADIUS server that is not linked to the selected RADIUS profile, or it was sent to a network interface that does not correspond to the selected server, SMG will ignore such a request. A call is made from a virtual number. Call routing is performed on general basis, via a dial plan linked to a virtual number.

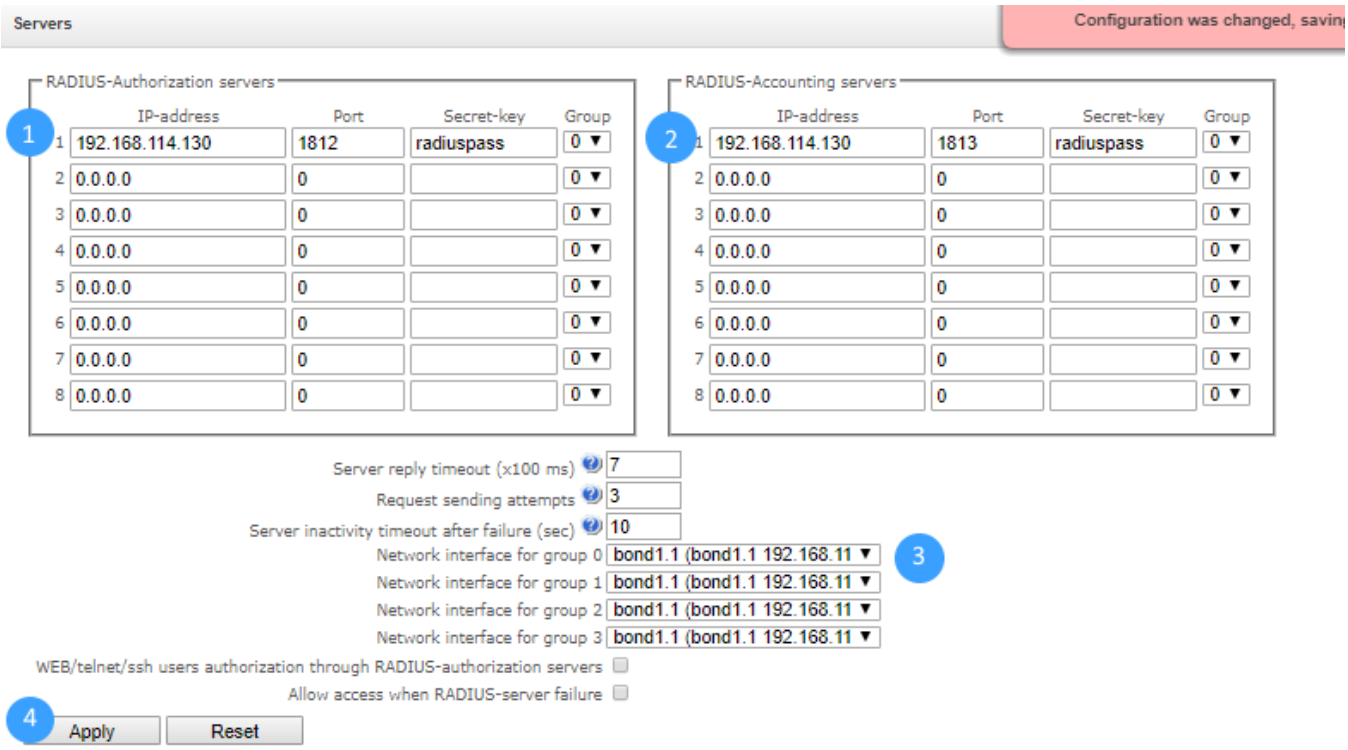
Virtual number parameters:

- PBX profile – PBX profile link;
- RADIUS profile – a profile that will be used to send Accounting requests. RADIUS CoA requests from servers linked to this profile can be accepted;
- Dial plan – dial plan link for call routing;
- Access category – access category selecting;
- Calling party category – calling line identification category selecting;
- Select mode – method of selecting numbers from a number pool:
    - random – numbers will be selected in random order;
    - sequential – numbers will be selected in order;
- Number pools – pools from which numbers for call making will be selected. To organize a pool, First number and Range should be specified. The maximum number of pools is 64.

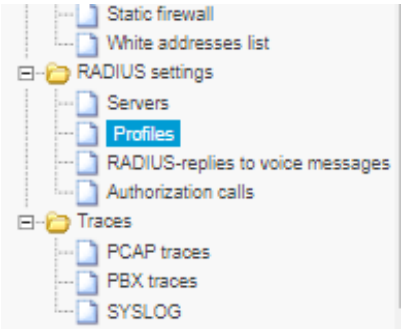
To configure the service:
Open the section "RADIUS settings -> Servers"



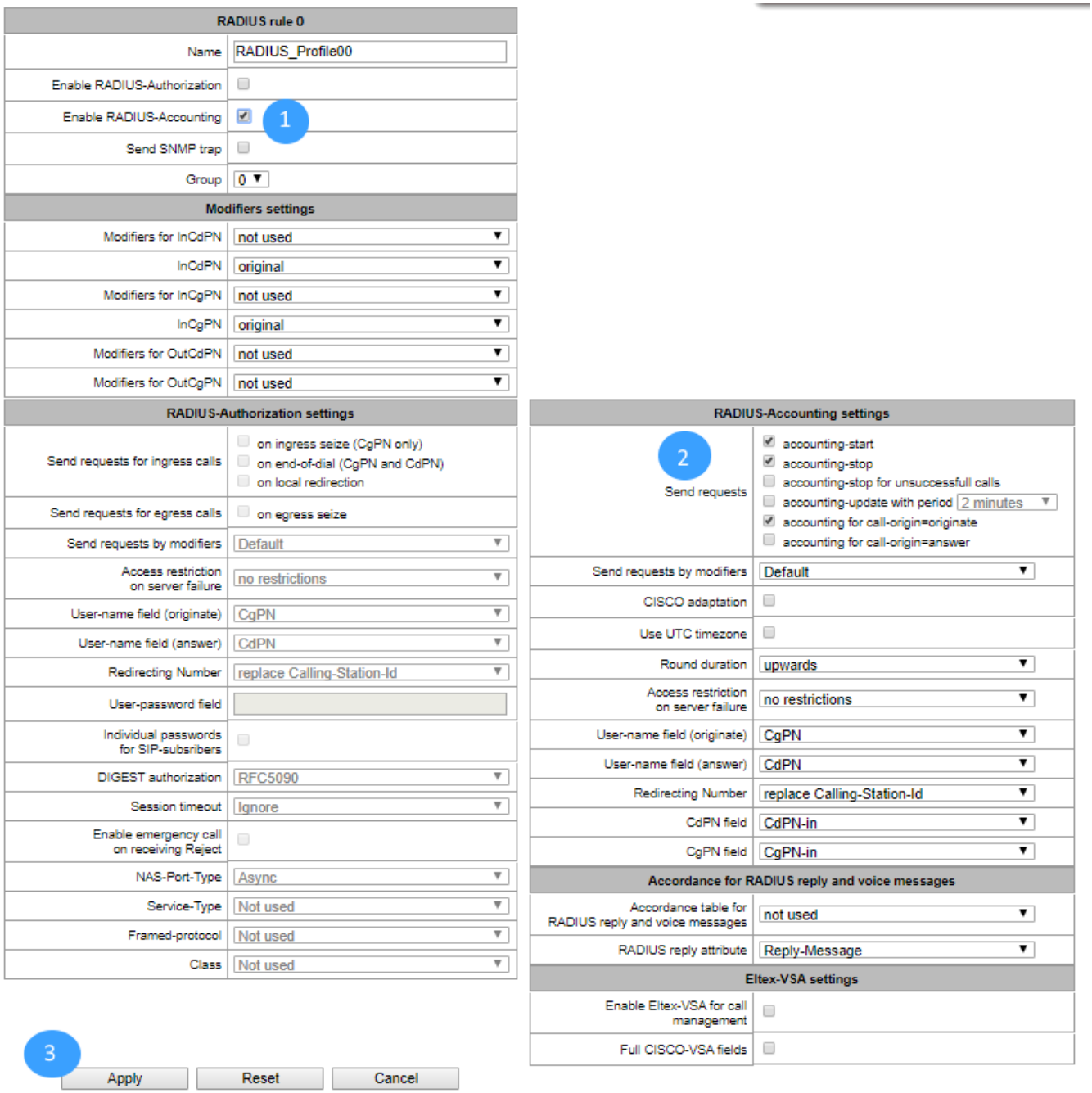
1 - Specify an address of a server from which a RADIUS CoA request will be sent;
1 - Specify an address of a server to which RADIUS Accounting will be sent;
3 - Choose a network interface that will be used for interaction;
4 - Apply the changes.



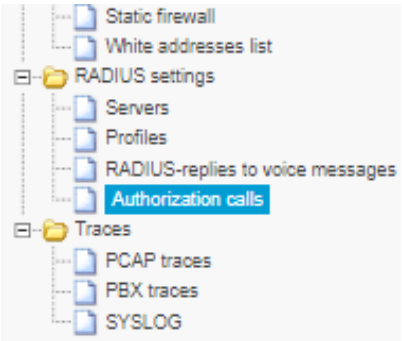
Open the section "RADIUS settings -> Profiles"



1 - Enable the option "Enable RADIUS-Accounting";
2 - Select events on which RADIUS Accounting requests will be sent;
3 - Apply the changes.



Open the section "RADIUS settings -> Authorization calls"



1 - Specify parameters for a virtual subscriber on whose behalf calls will be initiated;

- select PBX profile;
- select the RADIUS profile created before;
- specify a dial plan that will be used to make a call;
- specify Access catefory (if needed);
- specify Calling party category;
- specify Select mode - random or sequential one;
  2 - Add number pools that will be used to make a call. Specify First number and Range;
  3 - Apply the changes.