# v1.14_SoftWLC (EN)

Operation manual

# Contents

General features ..... 16
SoftWLC main modules ..... 17
Typical applications ..... 19
System requirements for the SoftWLC server ..... 22
v1.14_Datasheet SoftWLC (EN) ..... 23
General features ..... 23
Key features of SoftWLC ..... 23
Main SoftWLC modules and their functions ..... 23
System requirements for the SoftWLC server ..... 25
Minimum requirements for a system operator's work station ..... 26
v1.14_Installation and configuration instructions (EN) ..... 27
v1.14_Quickstart (EN) ..... 27
v1.14_Quickstart for Access points initialization ..... 27
v1.14_Quickstart for configuring Hotspot with portal authorization ..... 35
v1.14_Quickstart for configuring a Wi-Fi Enterprise network ..... 50
v1.14_SoftWLC installation and update (EN) ..... 59
v1.14_Step-by-step SoftWLC installation guide (the example for v1.7) ..... 59
Preparing for installation ..... 60
Installation ..... 62
Installing the license for Eltex EMS ..... 70
v1.14_Step-by-step SoftWLC installation using the installation script ..... 71
Preparing for installation ..... 71
Installation ..... 71
v1.14_Recommendations after installation of SoftWLC ..... 73
v1.14_SoftWLC multihost system installation ..... 75
Installing the ELTEX-PORTAL module ..... 75
Installing the ELTEX-WIFI-CAB module ..... 76
Installing the ELTEX-PORTAL-CONSTRUCTOR module ..... 77
Installing the ELTEX-APB module ..... 78
v1.14_SoftWLC backup (EN) ..... 79
General information ..... 79

Installing and configuring keepalived ..... 80
Configuring rsync ..... 80
Starting/stopping procedure ..... 80
Configuring rsync server ..... 81
Configuring synchronization launch ..... 83
Configuring MySQL replication ..... 85
Data dump transfer and transfer to the second server ..... 85
MySQL configuration ..... 85
Creating user accounts ..... 87
Starting replication ..... 87
Configuring MongoDB ..... 92
replicaSet configuration ..... 92
Eltex-PCRF operation in cluster mode ..... 94
Configuring PCRF cluster ..... 94
Configuring SoftWLC modules ..... 96
Changing configuration via GUI ..... 112
Admin Panel ..... 112
Portal Constructor ..... 113
EMS-GUI ..... 117
v1.14_keepalived_1.3.6 (EN) ..... 119
Package description ..... 120
Installation ..... 120
Starting/stopping procedure ..... 120
Configuration ..... 121
Saving a log to a separate file ..... 127
v1.14_Configuring SSID password change report sending (EN) ..... 127
v1.14_Integration with HotWiFi (EN) ..... 128
Access point firmware ..... 129
Setting up connection between the advertising platform and an access point ..... 129
Setting up connection between the advertising platform and BRAS ..... 132
v1.14_Integration with ESIA (EN) ..... 137
v1.14_Using TLS certificates for user authorization (EN) ..... 140
Generating a server certificate ..... 140
Creating a TLS certificate at users ..... 141

Creating an Enterprise SSID with support for TLS ... 144
Installing a certificate to a client's device ... 149
v1.14_How to change a password for accessing Admin Panel_Portal Constructor (EN) ... 151
v1.14_How to configure option 43, and other DHCP configuration aspects (EN) ... 154
Configuring option 43 for automatic connection to SoftWLC (10 suboption) ... 154
Configuring option 43 for creating GRE tunnels between access points and ESR-1000 (suboptions 11 and 12) ... 155
Configuring option 43 for AP autoconfiguration (suboption 6) ... 155
Configuring option 43 for identifying carrier network area the access point belongs to (suboption13) ... 156
Configuring the class for IP address allocation depending on Relay Agent IP address ... 156
Configuring the class for IP address allocation depending on Vendor Class Identifier ... 156
v1.14_Setting up AP group monitoring on a node (EN) ... 158
v1.14_Configuring call back authorization (EN) ... 159
Interaction scheme ... 160
Description ... 160
Configuring call back authorization ... 161
Troubleshooting ... 161
Identification scenario ... 163
SMG configuration ... 163
v1.14_Configuring trap sending via Syslog protocol (EN) ... 168
v1.14_Setting tariffs for portal authorization (EN) ... 169
Creating a tariff with captive portal authorization ... 169
Script examples ... 169
Tariff with time limit ... 170
Tariff with traffic quota ... 170
Tariff with bandwidth limit that changes at certain intervals ... 171
Tariff with limited access to resources ... 174
Tariff with periodic bandwidth limit change ... 175
v1.14_Setting 'Rate limit' (DHCP traffic) on AP and ESR (EN) ... 177
v1.14_Setting daily limit for BRAS (EN) ... 181
Description ... 182
Creating URL lists ... 182
Creating a welcome list ... 182

Creating white_list ... 183
Creating services ... 184
Creating limit2h1Gb service ... 184
Creating the blocking service ... 185
Creating a PCRF scenario ... 188
Creating a limit scenario ... 189
Creating a tariff ... 189
Creating a limitTP tariff ... 189
CheckCronBrasVerticle update interval ... 191
How it works ... 191
Constraints ... 193
v1.14_Creating dynamic tunnels using ESR location configuration in a client node (EN) ... 194
General description ... 194
The classic scheme of node tree search for data tunnel establishment ... 194
Problems of defining an ESR for data tunnel establishing in a classic ESR search ... 196
The scheme of searching ESR for data tunnel establishment by location configuration in a node ... 197
Configuring ESR location in EMS ... 200
Occupancy monitoring of the node where ESR devices for data tunnel establishment are located ... 206
ESR location configuration principles ... 208
v1.14_Troubleshooting Guide (EN) ... 209
v1.14_Listing all cron events ... 209
v1.14_Troubleshooting of Wi-Fi users connections ... 211
v1.14_Troubleshooting of obtaining IP addresses by Wi-Fi users ... 215
Initial diagnostics ... 215
Checking a DHCP server ... 215
2.1 One of the subnetworks used is not specified ... 216
2.2 Pool vacant addresses exhaustion ... 216
Checking a DHCP relay ... 216
Debugging in the Scheme with GRE ... 216
Debug in the Scheme without GRE ... 218
Checking an access point ... 218
v1.14_Network diagnostics on ESR ... 219

Check for the core availability from access point management networks ..... 219
Check for tunnels ..... 219
Interface traffic check ..... 220
Check for the DHCP availability from user network ..... 221
Check for external resources availability from a user network bridge ..... 221
v1.14_ISC DHCP server pool range usage monitoring ..... 222
v1.14_tomcat service monitoring on the SoftWLC server ..... 223
v1.14_RADIUS debug obtaining ..... 225
v1.14_Eltex-portal error codes table ..... 227
v1.14_SoftWLC modules (EN) ..... 229
v1.14_APB (EN) ..... 229
Description ..... 229
Service management ..... 229
Configuration ..... 230
/etc/default/eltex-apb ..... 230
/etc/eltex-apb/apb.properties ..... 231
/etc/eltex-apb/ehcache.xml ..... 232
/etc/eltex-apb/hosts.json ..... 232
Configuring access points connection to APB ..... 234
v1.14_Auth Service (EN) ..... 235
Description ..... 236
Service management ..... 236
Configuration ..... 237
/etc/eltex-auth-service/sql.conf ..... 237
server = "localhost" ..... 238
#port = 3306 ..... 238
login = "eltexauthservice" ..... 238
password = "eltexauthpassword" ..... 238
The table is stored in eltex_auth_service database. It contains the addresses of clients that have rights to send user authorization requests. If a client is not included into the table, authorization requests will be ignored. When the contents of the table is changed, restart eltex-auth-serviceNAS table ..... 238
v1.14_Eltex Portal (EN) ..... 238
Description ..... 238
Service management ..... 239

Configuration ..... 240
/etc/eltex-portal/application.conf ..... 240
/etc/default/eltex-portal ..... 243
/etc/eltex-portal/log4j2.xml ..... 243
Log errors description ..... 245
v1.14_List of recommended browsers ..... 245
v1.14_OTT (EN) ..... 247
General scheme ..... 248
Quickstart ..... 248
General description ..... 249
Service Activator ..... 249
ESR ..... 255
Redundancy ..... 255
ESR connection scheme ..... 256
ESR redundancy scheme ..... 256
Access points ..... 257
Use case ..... 258
Message exchange diagram ..... 261
Configuration ..... 261
AP initialization ..... 261
ESR OTT ..... 265
OTT black list ..... 273
Deleting OTT link ..... 274
Shaper settings via the Admin Panel ..... 274
NBI for OTT management ..... 276
Annex 1. List of IPsec parameters in the OTT profile ..... 277
Annex 2. Description of errors returned by the Service Activator to access points ..... 278
Annex 3. ESR configuration example ..... 279
Troubleshooting ..... 302
Service Activator logs ..... 302
Viewing OTT information on access points ..... 302
Manual starting of the Service Activator's client part on an AP with debug enabled ..... 303
v1.14_ESR-10+OTT+(1.6.0) Configuration and connection. General information (EN) ..... 303
General information ..... 304

Preconfiguration ..... 306
Configuring connection and initialization using a default rule ..... 308
Connecting clients ..... 316
Appendices ..... 337
v1.14_MySQL (EN) ..... 363
Service management ..... 364
Configuration ..... 365
The number of connections ..... 365
Memory size ..... 365
Collecting rsyslog ..... 366
Checking replication ststus in GUI EMS ..... 366
Database connection number calculation depending on server load ..... 367
mysql server operation analysis using MySQLTuner ..... 368
v1.14_Configuring MySQL replication ..... 370
v1.14_Restoring replication ..... 376
v1.14_NBI (EN) ..... 377
Description ..... 378
Starting/stopping procedure ..... 378
Configuration ..... 378
/etc/eltex-radius-nbi/radius_nbi_config.txt ..... 378
Configuring hikari cp ..... 381
Command documentation ..... 381
v1.14_Notification GW (EN) ..... 381
Description ..... 381
Starting/stopping procedure ..... 381
Configuration ..... 382
/etc/eltex-ngw/notification.properties ..... 382
/etc/default/eltex-ngw ..... 384
Configuration files to connect SMS gateways ..... 385
v1.14_Configuring incoming call authorization (EN) ..... 385
v1.14_Configuring outgoing call authorization (RADIUS) (EN) ..... 387
v1.14_Sending SMS using a script ..... 388
v1.14_Sending messages via NGW ..... 389
v1.14_RADIUS (EN) ..... 390

Description ..... 390
Starting/stopping procedure ..... 390
Configuration ..... 391
/etc/eltex-radius/local.conf ..... 391
NAS table ..... 393
Logging ..... 393
v1.14_Proxying to other RADIUS servers ..... 395
Default configuration ..... 395
Proxying authorization to another (home) RADIUS server ..... 397
Proxying authorization and accounting to home RADIUS server ..... 397
Proxying authorization and accounting to multiple RADIUS servers ..... 399
Disabling home server's status check ..... 401
Sources ..... 401
v1.14_Rotation and accounting storage ..... 401
Automatic start configuration ..... 402
Configuration files ..... 403
Script logging ..... 405
Configuring e-mail notification ..... 405
Data selection when creating an archive ..... 406
v1.14_DHCP server (EN) ..... 406
Description ..... 406
Starting/stopping procedure ..... 407
DHCP server configuration ..... 407
Network settings ..... 408
ISC-DHCP-SERVER configuration ..... 409
DHCP-failover configuration ..... 415
OMAPI configuration ..... 416
v1.14_dhcp.leases files rotation ..... 417
dhcp.leases file rotation problems diagnostics ..... 417
Configuring file rotation on the server ..... 418
v1.14_Admin Panel (EN) ..... 419
General information ..... 422
Entering the system ..... 422
Interface description ..... 422

Navigation ... 422
Using filters ... 423
Export of information ... 424
Restricting control elements visibility ... 425
Managing expanded statistics modal dialogs ... 425
Working with tables ... 425
Admin Panel menu ... 426
Start page ... 426
Statistic of a provider ... 427
SMS Statistic ... 435
Hotspot/Enterprise statistics ... 438
Services and tariffs ... 446
Wi-Fi users ... 455
Access points ... 476
Event log ... 481
Wireless networks ... 483
Scheduler ... 491
Advertising platform ... 492
Settings ... 492
PCRF settings ... 492
Reference ... 497
Law information ... 498
v1.14_Admin Panel administration (EN) ... 498
Configuration files ... 499
GUI settings ... 500
Licensing ... 517
v1.14_Description of Admin Panel and Portal Constructor users' privileges (EN) ... 517
Role attributes ... 518
Description of the Admin Panel and the Portal Constructor users' default roles ... 522
Converting roles to the default set ... 522
v1.14_Resetting the password to enter the Admin Panel/Portal Constructor (EN) ... 525
v1.14_PCRF (EN) ... 525
Description ... 525
Service management ... 526
Configuration ... 527

/etc/default/eltex-pcrf ..... 527
/etc/eltex-pcrf/eltex-pcrf.json ..... 528
/etc/eltex-pcrf/hazelcast-cluster-network.xml ..... 533
v1.14_Description of log errors ..... 535
Invalid RADIUS Authenticator ..... 535
v1.14_Additional software (EN) ..... 535
snmpd ..... 536
Description ..... 536
Starting/stopping procedure ..... 536
Configuration ..... 537
tftp-hpa ..... 538
Description ..... 538
Configuration ..... 538
ntpd ..... 538
Description ..... 538
Starting/stopping procedure ..... 539
Configuration ..... 540
rsyslog ..... 540
Description ..... 540
Starting/stopping procedure ..... 540
Configuration ..... 541
v1.14_NGINX for single-host installations ..... 542
NGINX installation and configuration ..... 542
tomcat configuration ..... 542
v1.14_Authentication and authorization in MongoDB ..... 543
Congifuring authentication in a cluster ..... 543
User configuration ..... 543
v1.14_Schemes and algorithms (EN) ..... 546
v1.14_Algorithm for accounting processing ..... 546
v1.14_Algorithm for establishing GRE tunnels and getting IP addresses by access points ..... 546
v1.14_Algorithm for working with enterprise users on Eltex access points ..... 549
v1.14_Algorithm for working with portal users on Eltex access points ..... 550
v1.14_Algorithm for working with portal users when connecting via BRAS+PCRF ..... 552

v1.14_Authorization on the portal ..... 554
Account confirmation by an outgoing call or SMS ..... 554
v1.14_List of service ports ..... 554
v1.14_Interaction scheme of SoftWLC components ..... 557
v1.14_Interaction scheme for call back authorization ..... 558
v1.14_Portal Constructor (EN) ..... 558
Description ..... 559
Starting/stopping procedure ..... 560
Configuration ..... 560
/etc/eltex-portal-constructor/application.conf ..... 560
System settings in GUI ..... 562
Gallery ..... 571
Adding/updating images ..... 572
Deleting images ..... 573
Dashboard ..... 573
Customer Cab ..... 574
Portals ..... 574
Creating a new portal ..... 574
Copying a portal ..... 575
Common settings ..... 576
Language settings ..... 580
Scheduler settings ..... 581
Payment service ..... 582
Tariffs ..... 583
Appearance ..... 584
v1.14_Requirements to portal graphic resources (EN) ..... 596
Header image (logo) ..... 596
Top image (banner) ..... 596
Bottom image (banner) ..... 596
Right and left images (banners) ..... 597
Background ..... 597
Information on other elements (buttons, labels, etc.) ..... 597
Additional pages ..... 598
Language settings ..... 598

A layout of banners on a portal ..... 599
v1.14_MAC Checker (EN) ..... 601
Service installation ..... 602
v1.14_Jerry (EN) ..... 602
v1.14_Mercury (EN) ..... 603
v1.14_Bob (EN) ..... 605
Service description ..... 605
Settings ..... 607
v1.14_Disconnect (EN) ..... 610
Service description ..... 610
Description of work ..... 611
Configuration ..... 612
v1.14_Doors (EN) ..... 613
Description ..... 613
Configuration ..... 615
v1.14_Logging (EN) ..... 616
v1.14_WIDS (EN) ..... 617
Licensing ..... 618
Enabling the service on APs ..... 619
Service configuration on access points and low-level logic ..... 619
eltex-wids-service configuration ..... 622
v1.14_Unsafe configuration criteria ..... 623
v1.14_SoftWLC licenses and certificates (EN) ..... 625
EMS device licenses ..... 625
Purpose ..... 625
Licensing procedure and installation ..... 625
Verification ..... 626
Admin Panel licenses ..... 626
Purpose ..... 626
Licensing procedure and installation ..... 627
Verification ..... 627
PCRF licenses ..... 627
Purpose ..... 627

Licensing procedure and installation ..... 627
Verification ..... 628
RADIUS certificates ..... 628
Purpose ..... 628
Licensing procedure and installation ..... 628
Verification ..... 629
GUI EMS certificates ..... 629
Purpose ..... 629
Licensing procedure and installation ..... 629
Verification ..... 629

- General features
- SoftWLC main modules
- Typical applications
- System requirements for the SoftWLC server

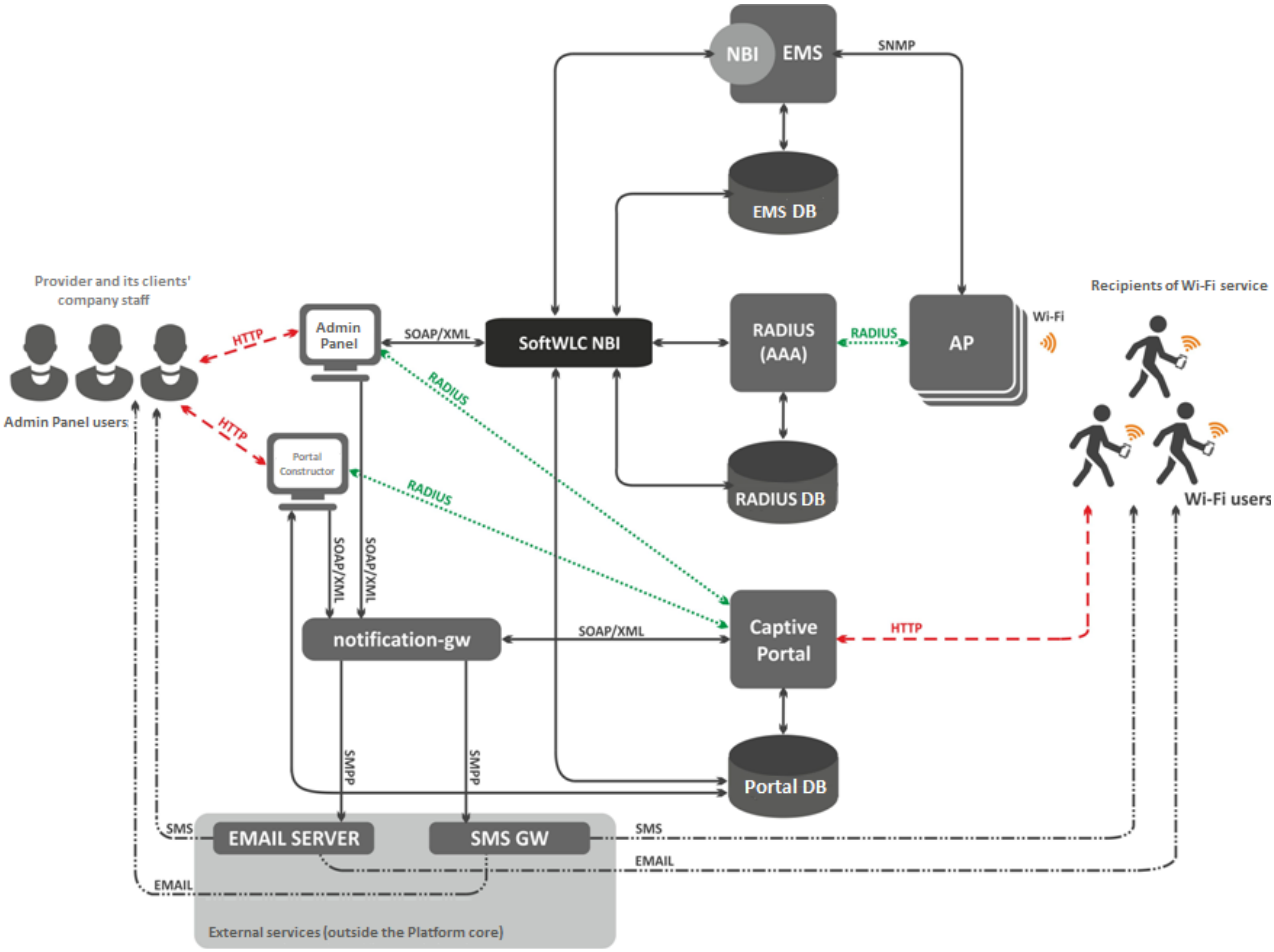
# General features

SoftWLC **is a software Wi-Fi controller** that consists of several modules performing various operations in order to provide complex solution for organization of centralized Wi-Fi networks with Portal and Enterprise authorization.  According to project requirements, certain modules can be included into the system or excluded from it.

**Key features of SoftWLC:**

- Control and monitoring of Eltex equipment that forms the basis of Wi-Fi solutions.
- Flexible administrative access policies distribution for various objects and features to be provisioned to SoftWLC users within a carrier's distributed hierarchy
- Hotspot service implementation with portal authorization that allows:
    - Integration of advertising providers' resources into a portal
    - Integration with payment systems
    - Portal design branding according to a client's requirements
- Enterprise authorization
- Possibility of integration with the external Active Directory
- Providing end users with a WEB tool for service management, portal branding and user account creation.
- SSID scheduling

# SoftWLC main modules

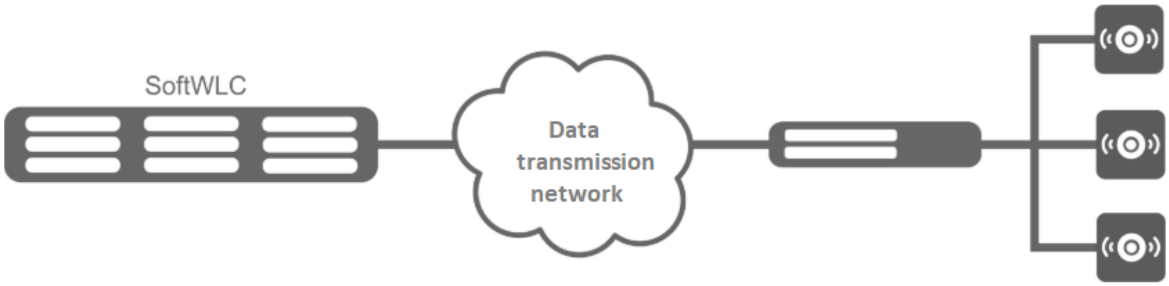



- **EMS-server** is a SoftWLC central component that provides management and monitoring of other modules of the system, GUI for an operator to work with SoftWLC and NBI interface for integration to a carrier's OSS.
- **WEB portal** is a module based on tomcat6 WEB server and providing a set of WEB portals for user authorization in Hotspot networks and Portal Constructor for their customization. The list of the WEB portal's features includes integration with SMS gateways and auto generation of Wi-Fi user accounts in a database.
- **B2B Admin Panel** is a WEB resource that provides a user with convenient interface for new Wi-Fi users' accounts creation and basic service management operations like SSID name change.
- **Database** – SoftWLC single database built on Mysql. Contains all the information about the system: from equipment configuration to user activity statistics.
- **RADIUS server** based on freeRADIUS is a module responsible for AAA operations (Authentication, Authorization, Accounting).
- **DHCP server** is a module that issues addresses for access points and Wi-Fi users. The server is based on isc-dhcp server. An operator can optionally use custom DHCP servers.
- **APB service** is a service intended for centralized synchronization of users' status information between access points. It provides seamless roaming between Hotspot access points.

- **Auth Service** is a common module for user authentication and authorization. Based on the RADIUS server. The service is used for authentication and authorization in the systems: B2B Admin Panel and WEB portal.
- **Notification Gateway** provides centralized communication between platform components and external systems that allow sending SMS and Email. The module interacts with B2B Admin Panel and WEB portal.
- **PCRF** is used for SoftWLC and ESR-1000 interaction in BRAS mode, when ESR-1000 implements Internet access policies for Wi-Fi subscribers and redirects users to an authorization portal.

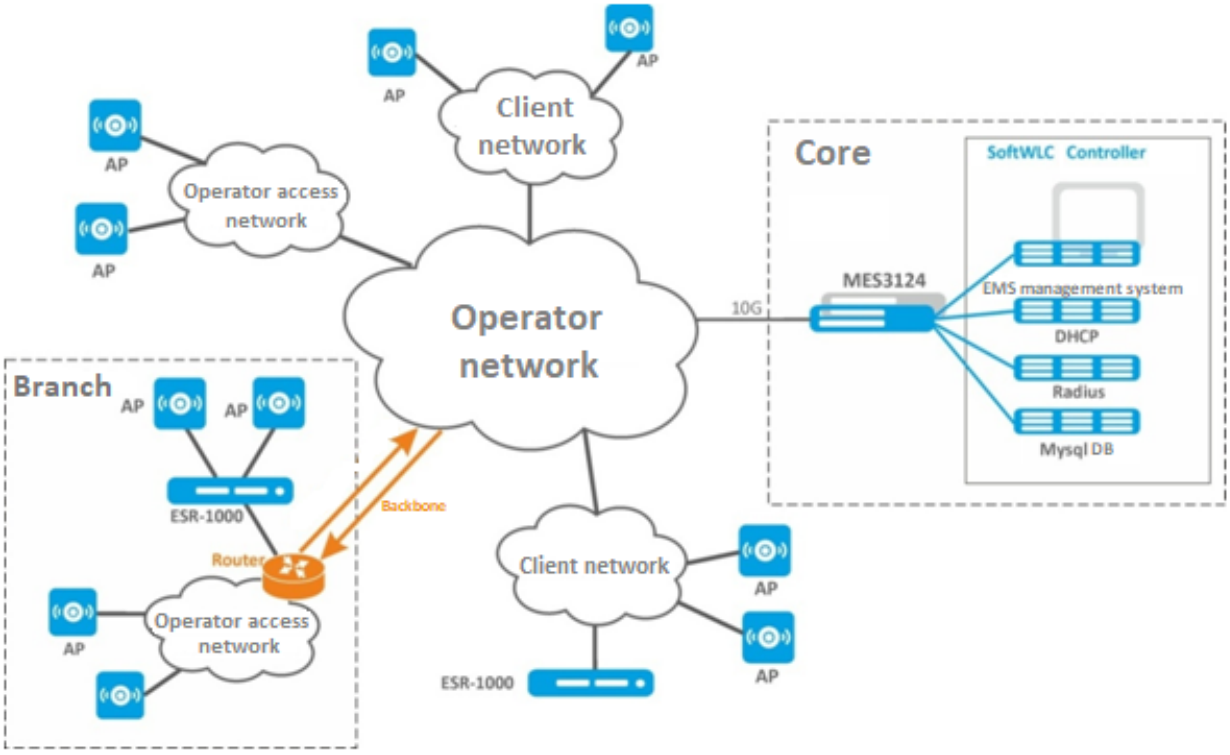
# Typical applications

**Minimal scheme**




Minimal solution requires two servers: each server includes all the modules with Active-Active redundancy. SoftWLC servers are integrated to an operator's network. L3 connectivity is provided between the servers and access points. That is enough to use the product. Management interfaces are configured on each access point to provide interaction with SoftWLC within a special control VLAN. Client data goes from access points in clients' VLANs (one VLAN for each SSID) to carrier network and then to the Internet.

**Global distributed scheme for large carriers**




This scheme is a case for large distributed networks deployed between several cities or regions. The number of servers required for SoftWLC operation depends on the planned traffic load. 10 servers are

needed for the maximum solution: the first pair of servers is reserved for EMS, WEB portal and APB, the second pair – for Database, the third pair – for RADIUS, the fourth pair – for DHCP. It is recommended to install Customer Cabinet to a separate redundant front-end server with maximum security. All the servers are connected to a pair of stacked switches that are connected to a redundant pair of routers in a carrier network. If a client decides to terminate subscriber sessions on his own territory, it is possible to move one or more ESR-1000 routers to a client's network. If a carrier network has global distributed backbone structure, it is possible to move ESR-1000 routers to subsidiaries.

**Scheme using ESR-1000 service routers**

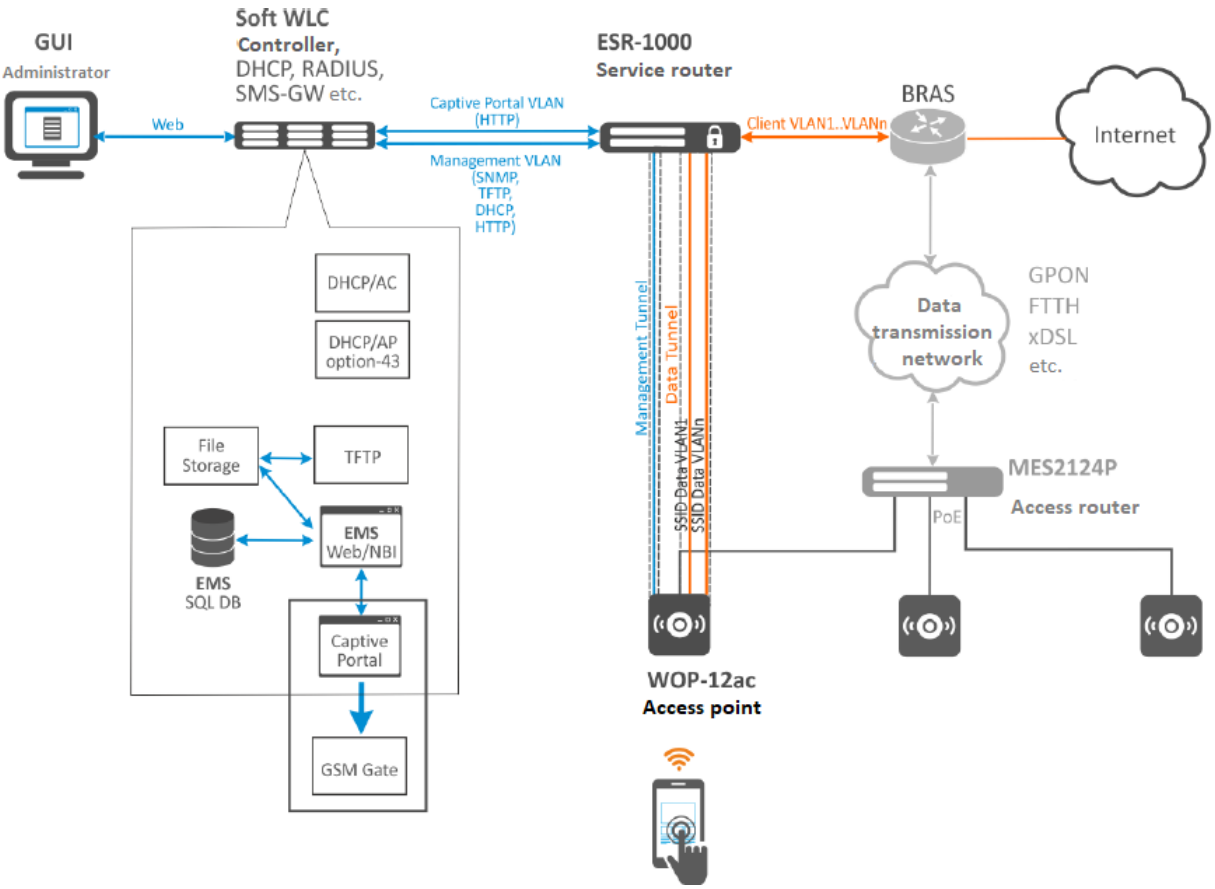
ESR-1000 service routers are used to solve the next tasks:

- relieving carrier network from subscriber session termination load;
- organization of automatic tunnel creation (L2 over GRE) between ESR-1000 and access points. The need for tunnel creation is to isolate subscriber traffic from management one. Due to the use of tunnels, an access point can be connected both to a client's or to a third-party access network and to interfaces that operate in "access" mode when processing L2 headers;
- network security organization by configuring a firewall integrated in ESR-1000;
- NAT (optionally);
- VRF implementation.

Access points can be connected both to a carrier's access network and to a client's one. When enabled, access points create Soft-GRE tunnels to ESR-1000 service routers over a carrier network. Then data is routed to SoftWLC or to the Internet.

SoftGRE tunnels between ESR-1000 and access points are created over a carrier L3 structure. Each access point has two tunnels: The *Management tunnel* for management traffic and the *Data tunnel* for subscriber traffic transmission.

The *Management tunnel* is used to transfer management traffic from/to an access point located in a separate management network. This subnet is invisible for a carrier's L3 segment due to *GRE tunnel* headers. Subscriber traffic is transffered within the *Data tunnel*. The traffic is terminated to ESR-1000 and then routed to a carrier network (to its NAT).


GUI
Administrator
Web
Soft WLC
Controller,
DHCP, RADIUS,
SMS-GW etc.
Captive Portal VLAN
(HTTP)
Management VLAN
(SNMP,
TFTP,
DHCP,
HTTP)
ESR-1000
Service router
Client VLAN1..VLANn
BRAS
Internet
DHCP/AC
DHCP/AP
option-43
File
Storage
TFTP
EMS
Web/NBI
EMS
SQL DB
Captive
Portal
GSM Gate
Management Tunnel
Data Tunnel
SSID Data VLAN1
SSID Data VLANn
Data
transmission
network
GPON
FTTH
xDSL
etc.
MES2124P
Access router
PoE
WOP-12ac
Access point

# System requirements for the SoftWLC server

SoftWLC software controller should be installed on a server with **Ubuntu Server 14.04 LTS** operating system

Technical support is carried out only with **Ubuntu Server 14.04 LTS** operating system

When choosing a server, the following system requirements should be taken into account:

| The number of devices | HP Proliant | CPU core, Xeon | RAM, Gb | HDD |
|---|---|---|---|---|
| **up to 50 AP*** | DL20 | 4, E3-1240v5, 8M Cache, 3.50 GHz | 8 | 2x500G |
| **from 50 to 200 AP** | DL60 | 6, E5-2603v3, 15M Cache, 1.60 GHz | 16 | 2x500G |
| **from 200 to 500 AP** | DL160 | 8, E5-2630v3, 20M Cache, 2.40 GHz | 32 | 2x1T |
| **from 500 to 1 thousand AP** | DL160 | 8, E5-2630v3, 20M Cache, 2.40 GHz | 64 | 2x1T |

# v1.14_Datasheet SoftWLC (EN)

## General features

SoftWLC is a software Wi-Fi controller that provides a complex solution for organizing guest and service networks. SoftWLC software package combines Wi-Fi access points, access switches and routers manufactured by Eltex into a single product. The package allows configuring and maintaining networks and user services in accordance with a client's requirements.

## Key features of SoftWLC

- Automated launching of access points
- Providing functions for monitoring of network elements: access points, access switches, routers
- Providing functions for network element individual control
- Providing functions for network element group control
- Providing functions for group policies, customer lists, individual/group shapers configuring and other service functions management
- Providing access points' firmware automatic update
- Providing Captive Portal authorization of Wi-Fi users with different identification methods: incoming SMS, outgoing SMS, voice call, Government Services, vouchers, preconfigured accounts of mass events participants
- Opportunity to create flexible portal scenarios with time or traffic limits for users. Paid scenarios are also available.
- Possibility of identification portal to flexibly work on schedule
- Opportunity to set up scheduled network operation including password rotation for portal identification network primary connection
- Providing Enterprise authorization with traffic encryption. Identification can be performed with a login/password or with an integrated TLS certificate
- Possibility of "portal" user roaming between access points and user id keeping between sessions
- Providing a graphical provider console for management and monitoring system
- Possibility of deploying a supervisory-level system which means that some settings and monitoring functions can be transferred from a provider to a client in accordance with B2B
- Providing provider's enterprise clients with B2B Admin Panel graphical interface that comprises basic elements for obtaining network operation statistics and tools for Wi-Fi users' accounts management
- Providing enterprise clients with guest portal setting GUI (in accordance with B2B) that includes basic elements for design, identification options and other features
- Providing service interface (Northbound) for system settings automatization and connection with the provider's or its B2B clients' OSS

## Main SoftWLC modules and their functions

- **EMS server**
  - management and monitoring of other modules of the system
  - receiving and processing of SNMP traps sent by system components
  - device initialization and configuration

    - performing group operations with devices
    - notification on failures
    - scheduled monitors to control system operation
    - providing graphical user interface
    - monitoring with saving data to a Round-Robin Database
- **WEB portal**
    - A module providing a set of WEB portals for user authorization in Hotspot networks
- **Portal Constructor**
    - A tool that allows virtual portal creating and configuring for user authorization in Hotspot networks
- **B2B Admin Panel**
    - providing interface for Wi-Fi users' accounts creation and basic service management operations
- **Database**
    - Mysql
    - MongoDB
- **RADIUS server**
    - AAA operations
    - WPA-enterprise authorization
- **DHCP Server**
    - assigning primary (external) IP addresses to access points with option 43 (suboptions 11 and 12) that allows creating GRE tunnels to ESR
    - assigning secondary (management, tunnel) IP addresses to access points with option 43 (suboptions 10 and 13) for access point management, detection and automatic initialization
    - assigning IP addresses to Wi-Fi users connected to access points
    - classification of DHCP clients by 82, 60 options and giAddr Field
- **APB service**
    - roaming for users authorized via WEB portal
    - configuration and transmission of public IP address lists for portal authorization
- **Auth Service**
    - system authentication and authorization
        - B2B Admin Panel
        - Portal Constructor
- **Notification Gateway**
    - centralized interchange between platform elements and external systems (SMS gateways, Call centers and electronic mail servers) via SMTP, SMPP, HTTP, WebSocket
- **PCRF**
    - authorization and authentication of users connected via BRAS (the mechanism allows providing user service based on third-party vendors' access points)
    - accounting accumulation for all authorization mechanisms and transferring it to a database
    - controlling the number of Wi-Fi users' simultaneous sessions for all authorization mechanisms
    - deauthentication of Wi-Fi users authorized via WPA-enterprise modes and BRAS
- **NBI**
    - connection between SoftWLC components via the SOAP protocol
    - service operation maintenance
        - Customer Cab

        - Portal Constructor
        - PCRF
    - TLS authorizaton certificates issuing

**SoftWLC technologies:**

- equipment management and monitoring
    - SNMP
    - ICMP
- user authorization
    - portal authorization on Eltex access points
    - EAP authorization (WPA2 enterprise) on the RADIUS server
    - portal authorization on third- party access points (BRAS + PCRF)
- Roaming
    - portal user roaming on Eltex access points
- Integration with external systems
    - SMS gateways
        - SMSC gateway
        - PTK gateway
        - Sviazbank gateway
        - Svyaznoy Zagruzka
        - SevenSky
        - GSM gateways (NetPing SMS)
    - Active Directory
    - Hot-WiFi
    - ESIA

**Compliance of used technologies (protocols) with standards and specifications:**

- EAP (WPA2)
    - IEEE 802.11i ( Wi-Fi Protected Access II, defines security mechanisms for wireless networks)
    - AES (encryption standard)
    - RFC 3748
- SNMP
    - defined as a component of TCP/IP by the IETF
    - RFC 1157
- ICMP
    - is an Internet standard (included in the STD 5 standard)
    - RFC 792
- RADIUS
    - RFC 2866 RADIUS Accounting
- RRM
    - IEEE 802.11h - Transmit power control and dynamic frequency selection for wireless local area networks
    - IEEE 802.11k - RRM for wireless local area networks
- SMTP
    - RFC 5321
- HTTP
    - RFC 2616
- WebSocket
    - RFC 6455
- Roaming is carried out in accordance with IEEE 802.11r standard

## System requirements for the SoftWLC server

- Ubuntu Server 16.04 LTS **operating system**

| The number of devices | HP Proliant | CPU core, Xeon | RAM, Gb | HDD |
|---|---|---|---|---|
| **up to 50 AP** | DL20 | 4, E3-1240v5, 8M Cache, 3.50 GHz | 8 | 2x500G |

| The number of devices | HP Proliant | CPU core, Xeon | RAM, Gb | HDD |
|---|---|---|---|---|
| **from 50 to 200 AP** | DL60 | 6, E5-2603v3, 15M Cache, 1.60 GHz | 16 | 2x500G |
| **from 200 to 500 AP** | DL160 | 8, E5-2630v3, 20M Cache, 2.40 GHz | 32 | 2x1T |
| **from 500 to 1 thousand AP** | DL160 | 8, E5-2630v3, 20M Cache, 2.40 GHz | 64 | 2x1T |

## Minimum requirements for a system operator's work station

Dual core processor with 2.5 GHz or more frequency
Random access memory size 4 GB or more
Monitor resolution 1920x1080 or more
Stable server connection, recommended speed 10Mbit/s or more
Keyboard, mouse
java jre 1.8 (with relevant updates)
Chrome or Firefox browser (with relevant updates)

# v1.14_Installation and configuration instructions (EN)

## v1.14_Quickstart (EN)


- v1.14_Quickstart for Access points initialization
- v1.14_Quickstart for configuring Hotspot with portal authorization
- v1.14_Quickstart for configuring a Wi-Fi Enterprise network


## v1.14_Quickstart for Access points initialization

**1 Initial setup**

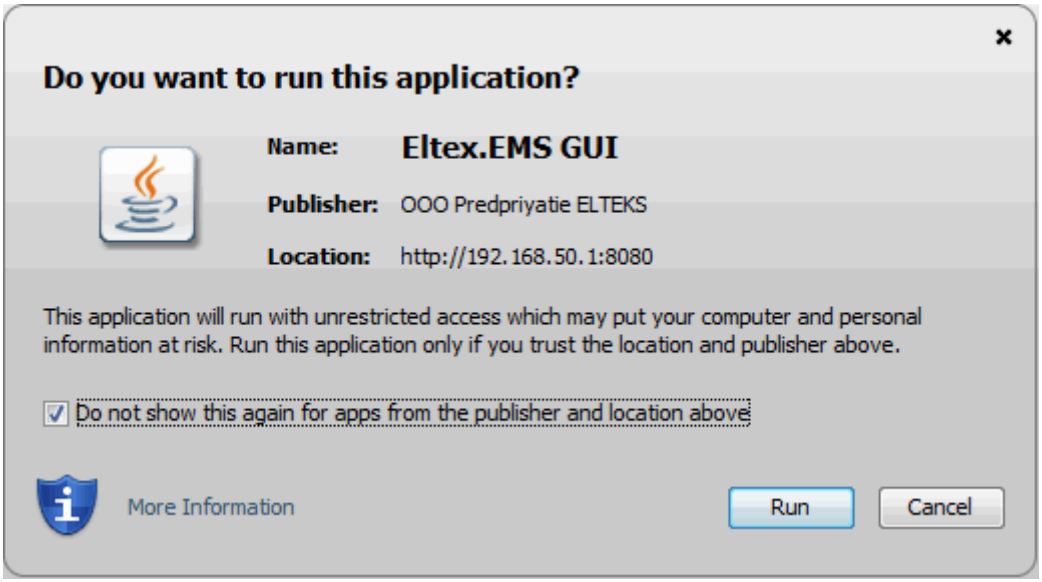
To open the EMS GUI, run the Java Web Start application (Oracle-Java8 must be installed).

1.1 Enter the server address in the browser address bar:

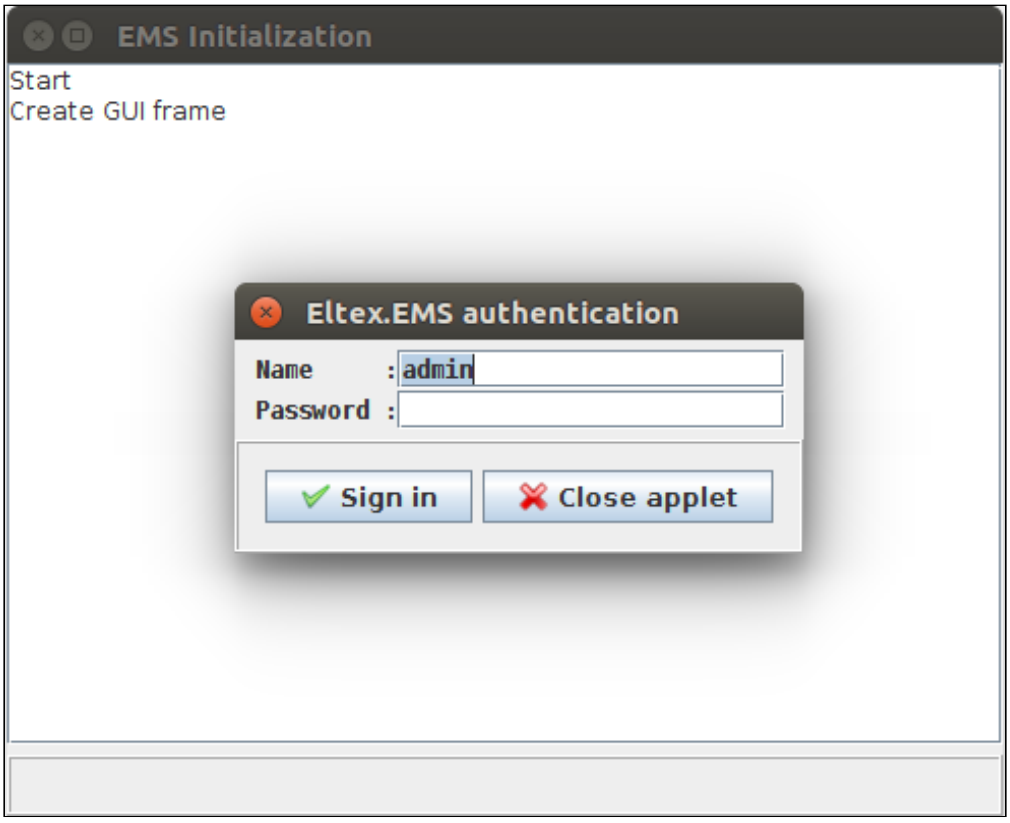
```
192.168.50.1:8080/ems/jws
```


To create a shortcut opening the EMS GUI on the desktop, you must enable temporary file storage in the Java Control Panel. Run the downloaded file having **.jnlp** format.

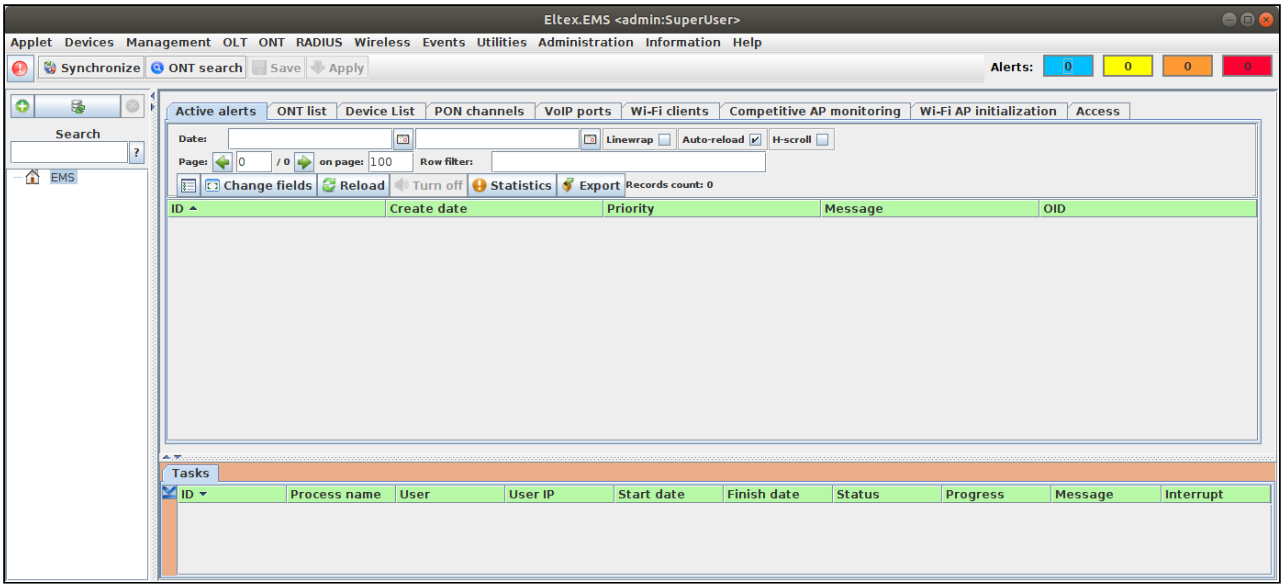
When loading a page, you may need a permission to run the Java application, as shown below. Select "Do not show this again for apps from the publisher and location above" and click "Run" button so that the message does not occur again.




1.2. For authorization on EMS server, enter the username **admin** without a password.




1.3. After authorization, the EMS GUI will open.

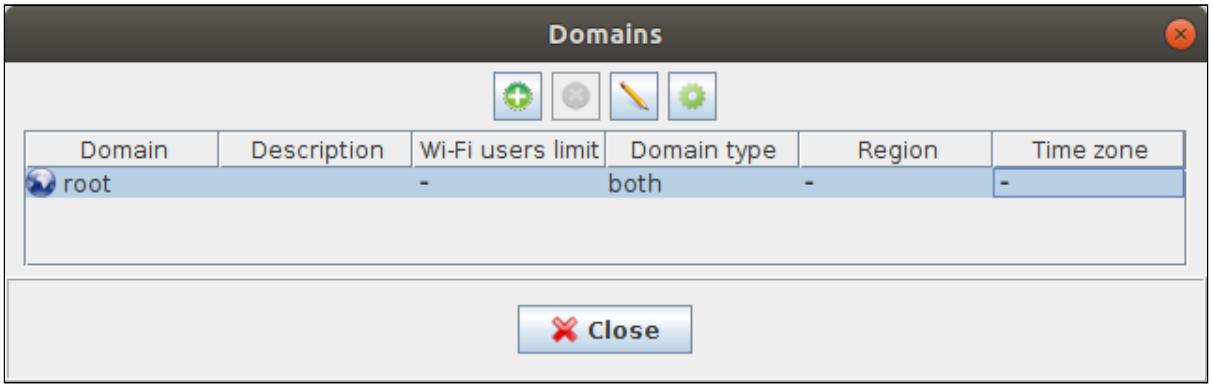



The main menu and controls are located under the window title.

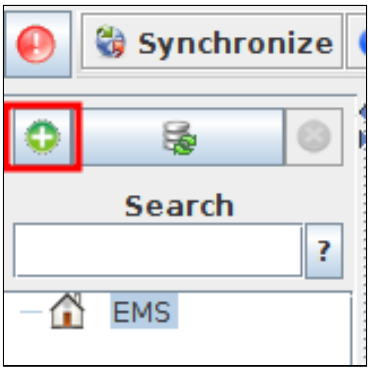
1.4. Perform the initial controller setup.
Go to **"Administration/Server configuration/System modules"** menu. Open **System** tab and specify:

- IP address of the EMS server in the control network of the station: **192.168.50.1**;
- Tomcat URL: **http://192.168.50.1:8080** (used for downloading files by EMS user);
- Internal Tomcat URL : **http://192.168.50.1:8080** (used for software updating via HTTP) ;
- type of device system access: **BY_DOMAIN**.

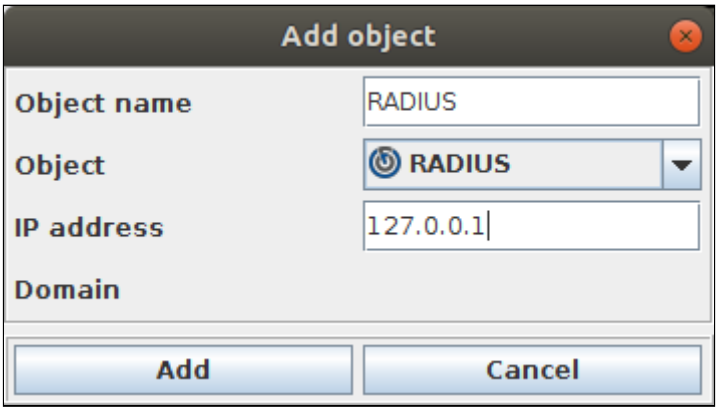
Click the "tftpserver" tab and save your changes. Set the IP address for the station devices: **192.168.50.1**. Click **Accept** and save changes you made.
Restart EMS by command **sudo service eltex-ems restart** or by using the **"Administration/Server configuration/EMS server Restart"** menu.
Create domains in the system. To do this, select **Administrative Tools**, then **Rights** and **Users**, and **Domains**. Create the root domain **root** and sub domains if necessary.




1.5 Add the RADIUS object to the object tree.
Click the **"+"** button in the Control Panel to add the object to the device tree.

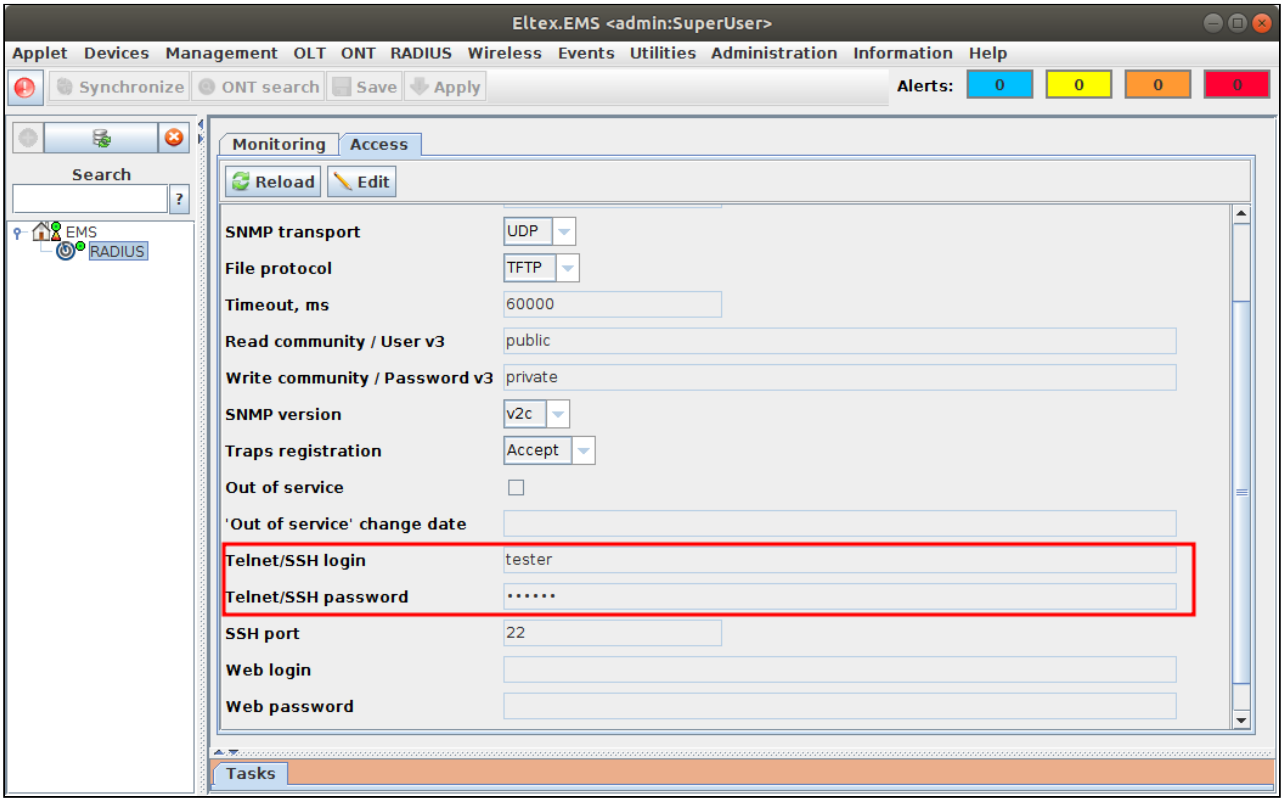



In the window that appears, enter the name of the object, select the type “RADIUS” and specify the IP address. If the RADIUS server is installed locally on your server, enter 127.0.0.1.




Click **Add**, then the RADIUS object appears in the object tree.
Select the **RADIUS** object in the tree and open the **Access** tab, click **Edit** and enter the login and password to access the server. In this case :

```
Telnet/SSH login: tester
Telnet/SSH password: tester
```

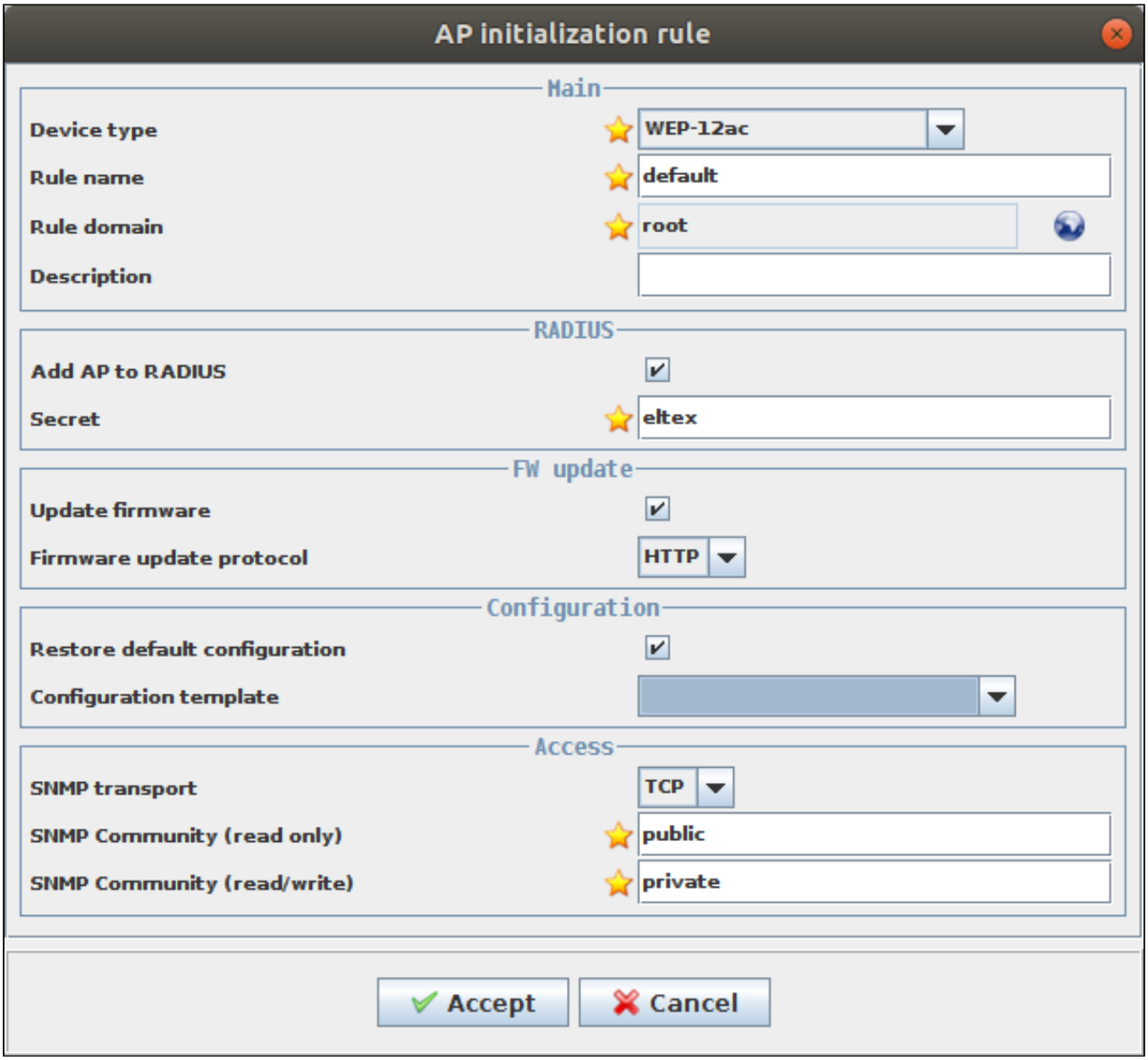



**2 Adding Access Points**

Connect the access point to the network according to the scheme. When enabled, the access point will receive a DHCP address. In order for the point to inform the controller about its presence in the network,

you must configure Option 43 with 10 DHCP suboption in which IP SoftWLC will be transmitted. Then the access point will automatically appear in EMS in the **Initialization of Wi-Fi AP** tab.

2.1. Create initialization rules in the **Wireless/Initialization Rules Manager of access points** menu . Add a rule, select a device type, specify the rule name and domain.

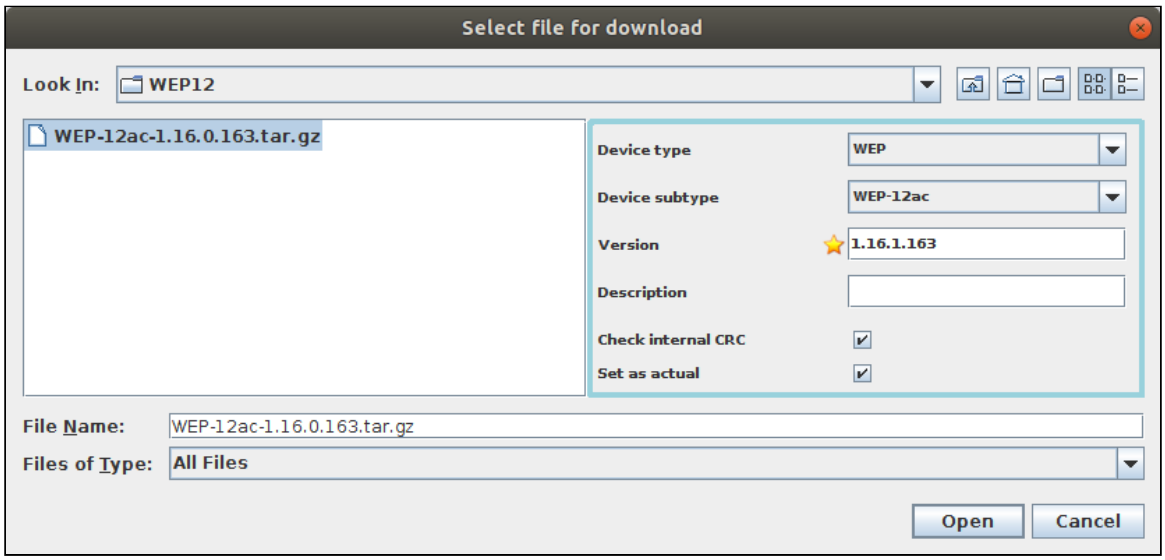



In the initialization rule

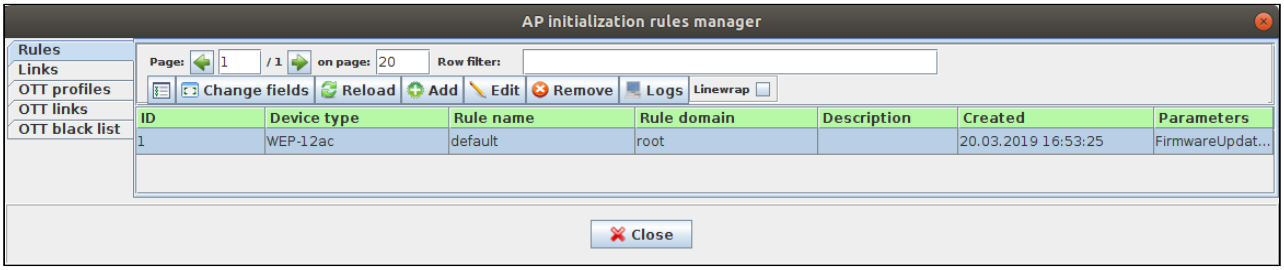
- You need to activate the addition of the AP to the RADIUS database and to specify the password of the AP to RADIUS: 'eltex' ('key' field). Otherwise, users will not be able to perform authentication.
- To automatically update the software on the AP during initialization, select the **Update to current software file** flag and select the software file transfer protocol (TFTP or HTTP).

  In order for the upgrade to be performed, you must download the latest software to the server before initializing the access points. To do this, use **" *Administration/Device firmware/Station***

***firmware"*** menu. The current software can be downloaded from the official website https://eltex-co.com/catalog/enterprise_wi-fi_access_point/. For each type of access points, you should download your own software file, and you should specify the device type and subtype when downloading. Set the **Make relevant** flag, to update the access point to the selected firmware version when initializing.



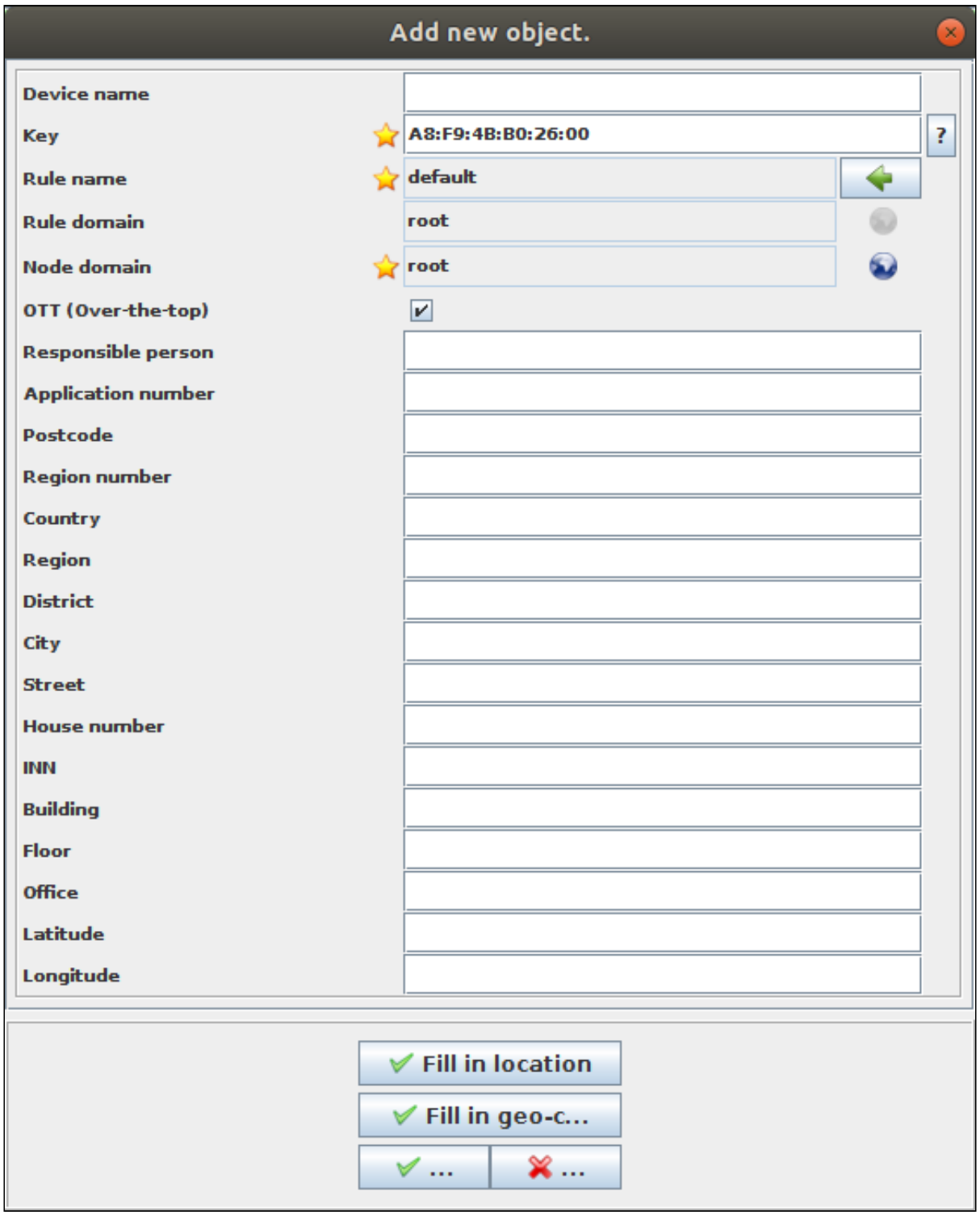

- To restore the default configuration on the access point before adding AP to the tree, set the **Restore Default Configuration** flag.
- You can select a pre-created configuration template (in the menu “Wireless/Configuration Template Manager”), which will be assigned to the AP. If necessary, create a template beforehand and select it when creating an initialization rule. Alternatively, edit the rule after creating the template.
- Select the protocol for SNMP packet transmission between the access point and EMS: TCP or UDP, as well as **Community** field values. Click **Accept** button, the created rule will be displayed in the AP initialization rules manager .



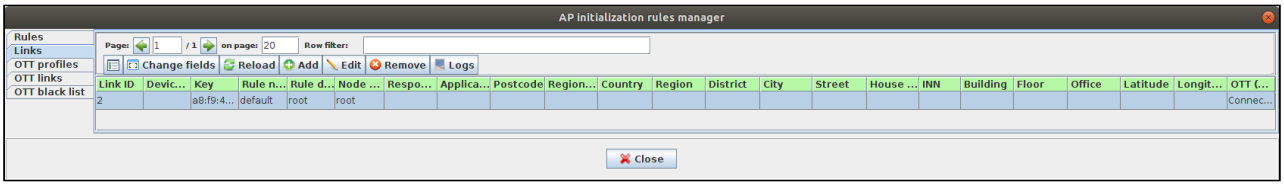

2.2. Configure the binding of the access point to the initialization rule. To do this, open the **Links** tab.

Binding can be performed by three types of keys: MAC address of the a ccess point, access point IP address (or IP address range), 13 suboption of 43 DHCP (location) option. If you specify **Device Name**, the access point appears with it in the tree. If you leave the field empty, MAC address and device type will be displayed as the name. You also need to specify the name of the initialization rule to bind (click  button at the end of the line to select from existing rules), the rule domain, and the host domain where

the access in the device tree. With a complex host domain hierarchy, all the required nodes will be created.

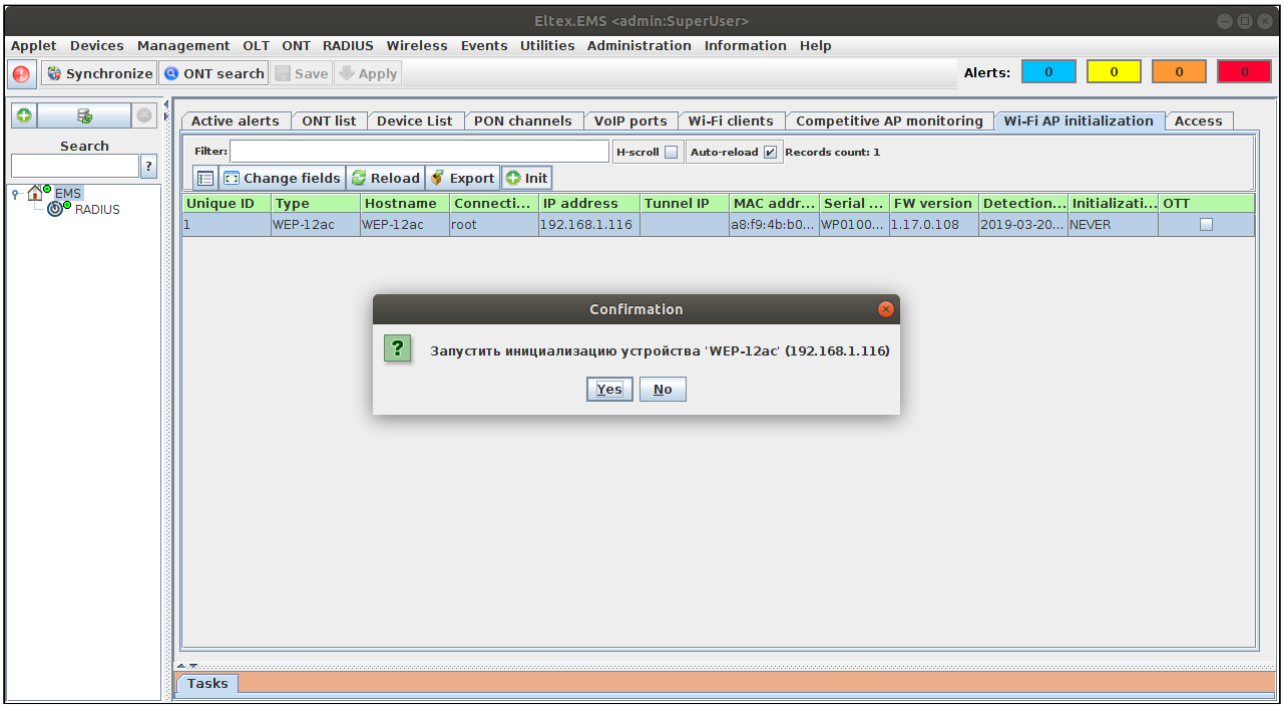



Created mapping will be visible in the AP initialization rule manager.

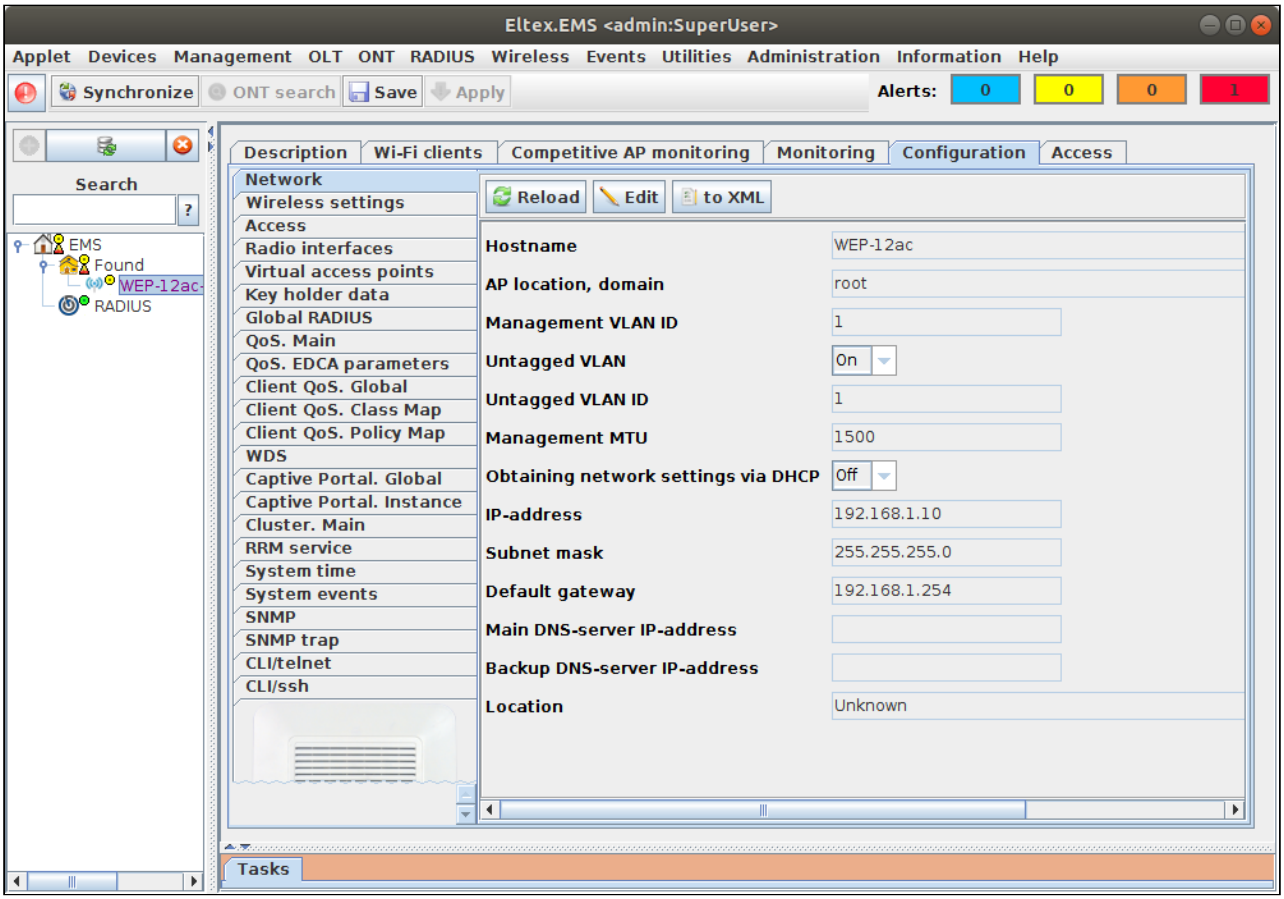



2.3. To initialize an access point with the specified parameters, select the root node in the left side of the window, open the **Wi-Fi AP Initialization** tab on the right side of the window, select the access point and click the **Initialize** button.

If the **Automatic Initialization** flag is set in the **"Administration/Server Configuration/System Modules"** menu in the **'WirelessCommon'** module, the initialization will be started automatically as soon as the corresponding binding is created.




Initialization process is displayed in the **Tasks** tab that you may open from the **Applet/View/Dashboard** menu or by pressing **Alt+F6** hotkey. When the process is finished, access point will be shown in the tree according to the initialization rule host domain.




## v1.14_Quickstart for configuring Hotspot with portal authorization

1. Enable the **Captive Portal** mode. To do this, select **Captive Portal. Global** in the **Configuration** tab, click **Edit** and select **On** for **Captive Portal Mode** option. Specify **Roaming service URL** in the next format: *ws://host:port/apb/broadcast*. Click **Accept**.

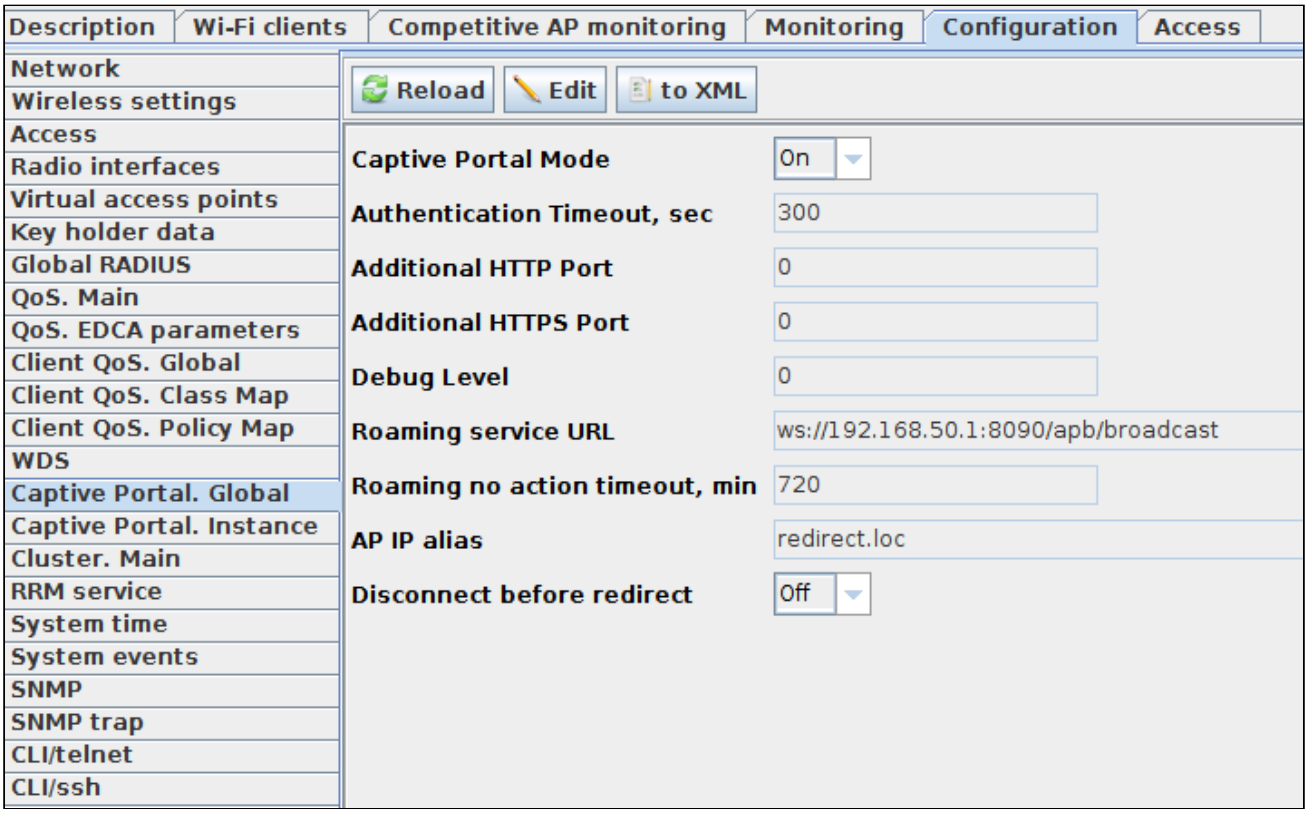



*Figure 1 – Captive Portal. Global setting*

This setting can be done by creating a configuration template in the **Wireless settings/Configuration template manager** and applying it to one or more access points.

2. Open the **SSID manager** and create a new SSID. Specify the following settings:

**Type = Hotspot**
**Name = Test_hotspot**
**Domain = root**
**VAP status = up**
**Security mode = w/o encryption**
**Status of Client QoS = on**
**VLAN-ID = 1000**
**RADIUS IP Address = 192.168.50.1**
**RADIUS key = eltex**
**Radius Accounting = Up**
**Set "Captive portal" - "Enabled"**
**Virtual portal name = default**[1]
**Verification = CaptivePortal**
**Set "External" checkbox**
**External URL = http://192.168.50.1:8080/eltex_portal/**

**User mobility domain = root**[2]

**Note**

VLAN-ID = 1000 is used as an example. It should be specified here the service VLAN that is actually used on Your network and comes to the access point. The DHCP server must be accessible for VLAN users.

Select the Radio interfaces to which the generated SSID will be assigned. If you assign an SSID to all radio interfaces simultaneously ("Radio" - "All"), it is recommended to enable" Band steer " (select check box) for priority connection to the 5 GHz network by devices that support both bands. When you assign SSID on one radio interface, **Band steer** mode should be off.

To optimize roaming, the minimal signal mechanism is used.

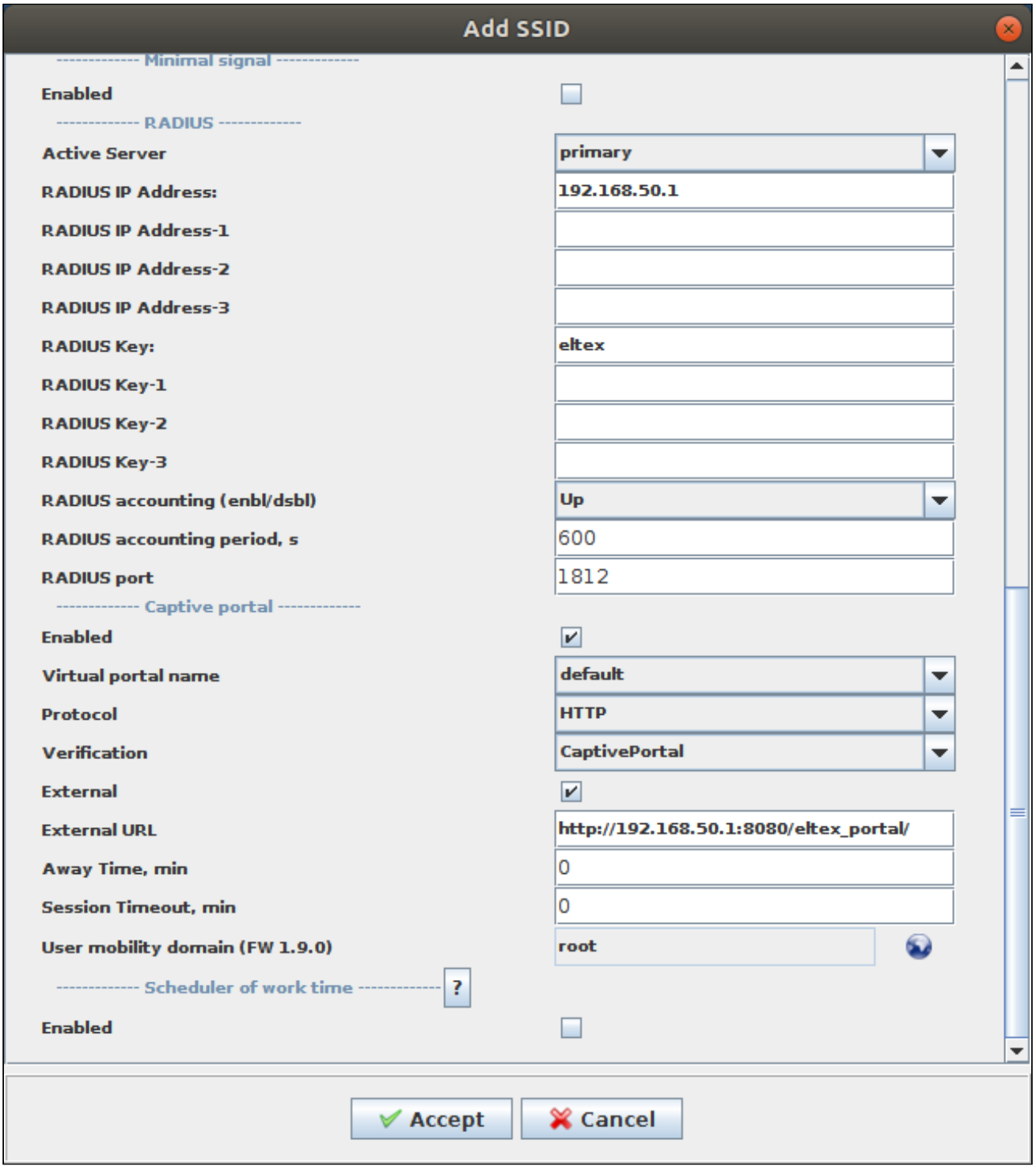



*Figure 2 – SSID settings*

In order for the client to be redirected to a specific page for authorization when connecting to Hotspot SSID, it is necessary to select the name of this page in the **Virtual portal name** field. Pages are pre-created in the portal, and then appear in the list and become available for selecting.

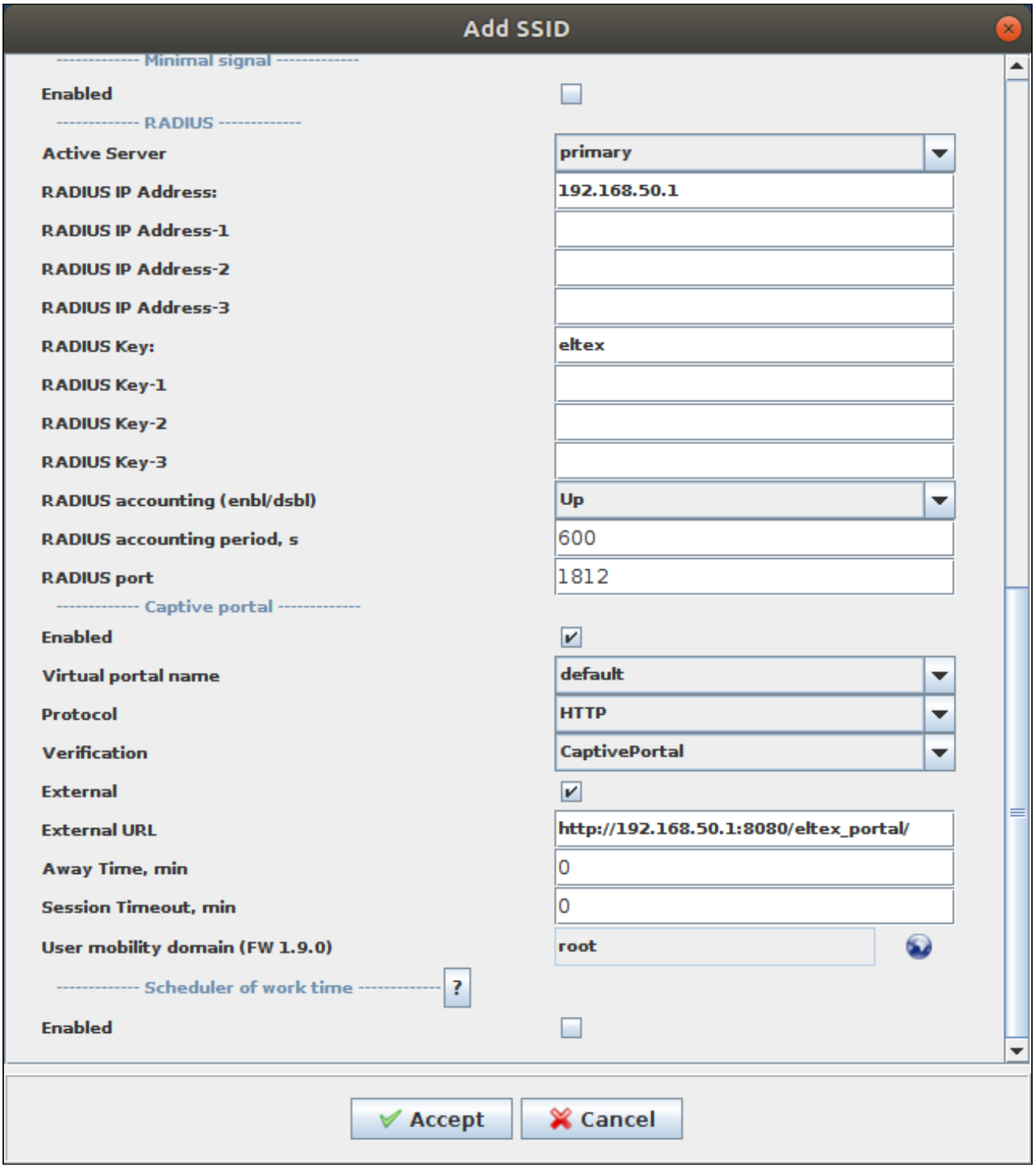



*Figure 3 – Settings of SSID Captive portal*

After clicking **Accept** button, the created SSID will appear in **SSID table** (Figure 4).

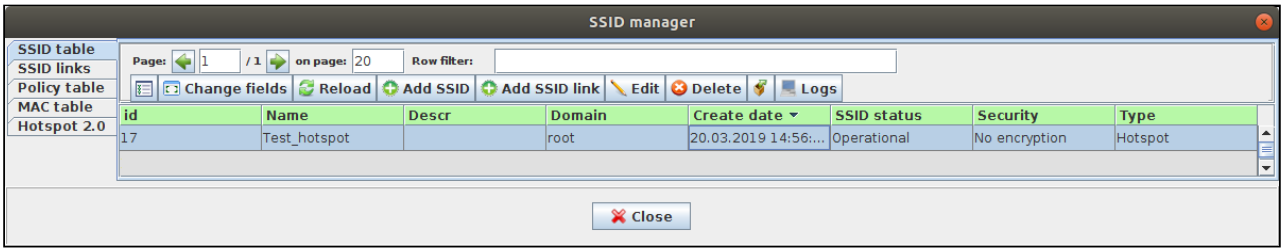



*Figure 4 – SSID manager*

3. Assign the SSID to the access point via the **Add SSID link** button.
The SSID will be assigned to the first disabled VAP on the access point. You can see the result in the **Configuration/Virtual access points** tab (see Figure 5).

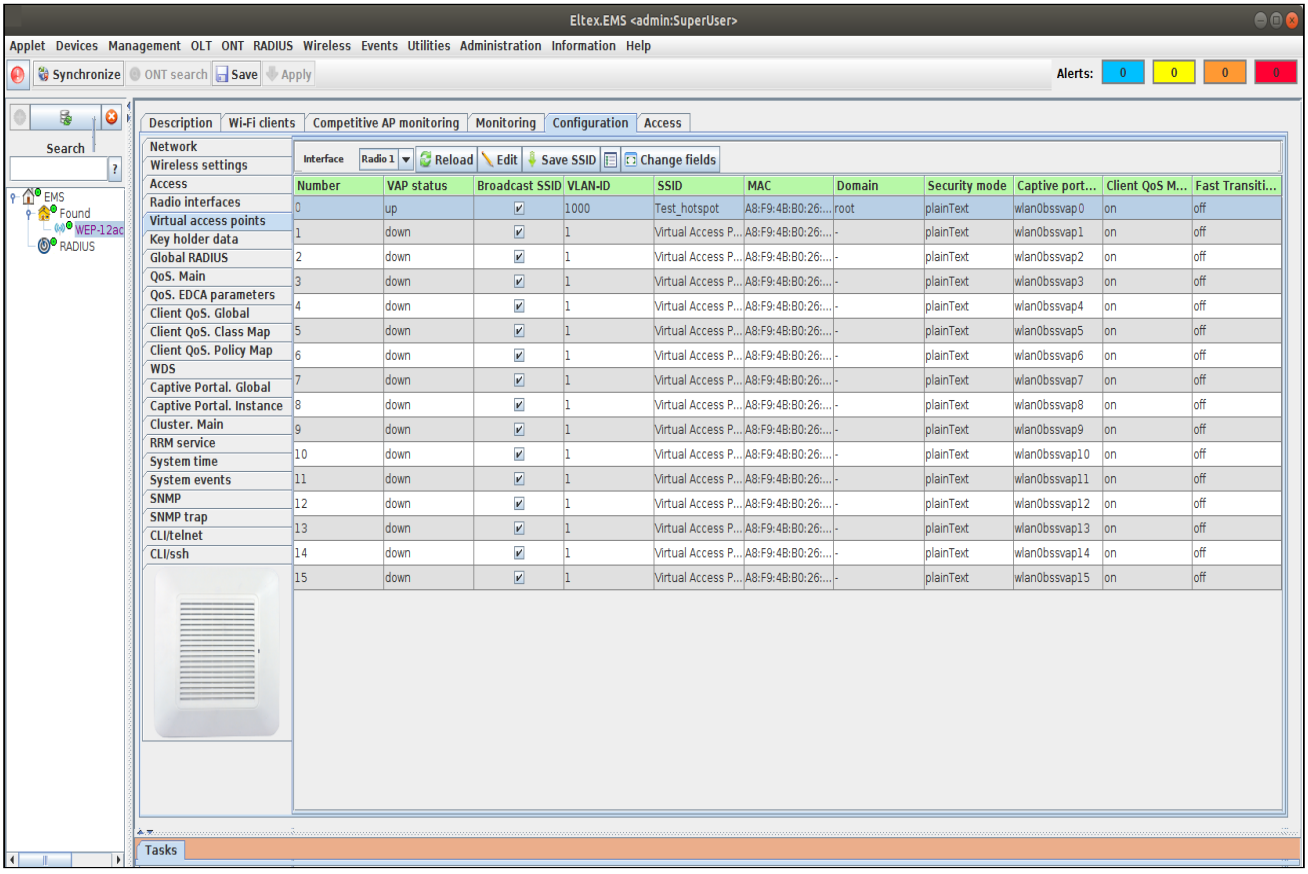



*Figure 5 – Virtual access points*

4. Add a tariff plan.
In the **RADIUS/New tariff settings** menu, click **Add** button and specify the basic tariff plan settings:

- Name: tarif1;
- Code: 2;

- Domain: root.

Set the **Portal auth** check box.

Examples of using tariff plans can be found in the article "SoftWLC. Tariff plan configuration for portal authorization" that is available on v1.14_Setting tariffs for portal authorization (EN)

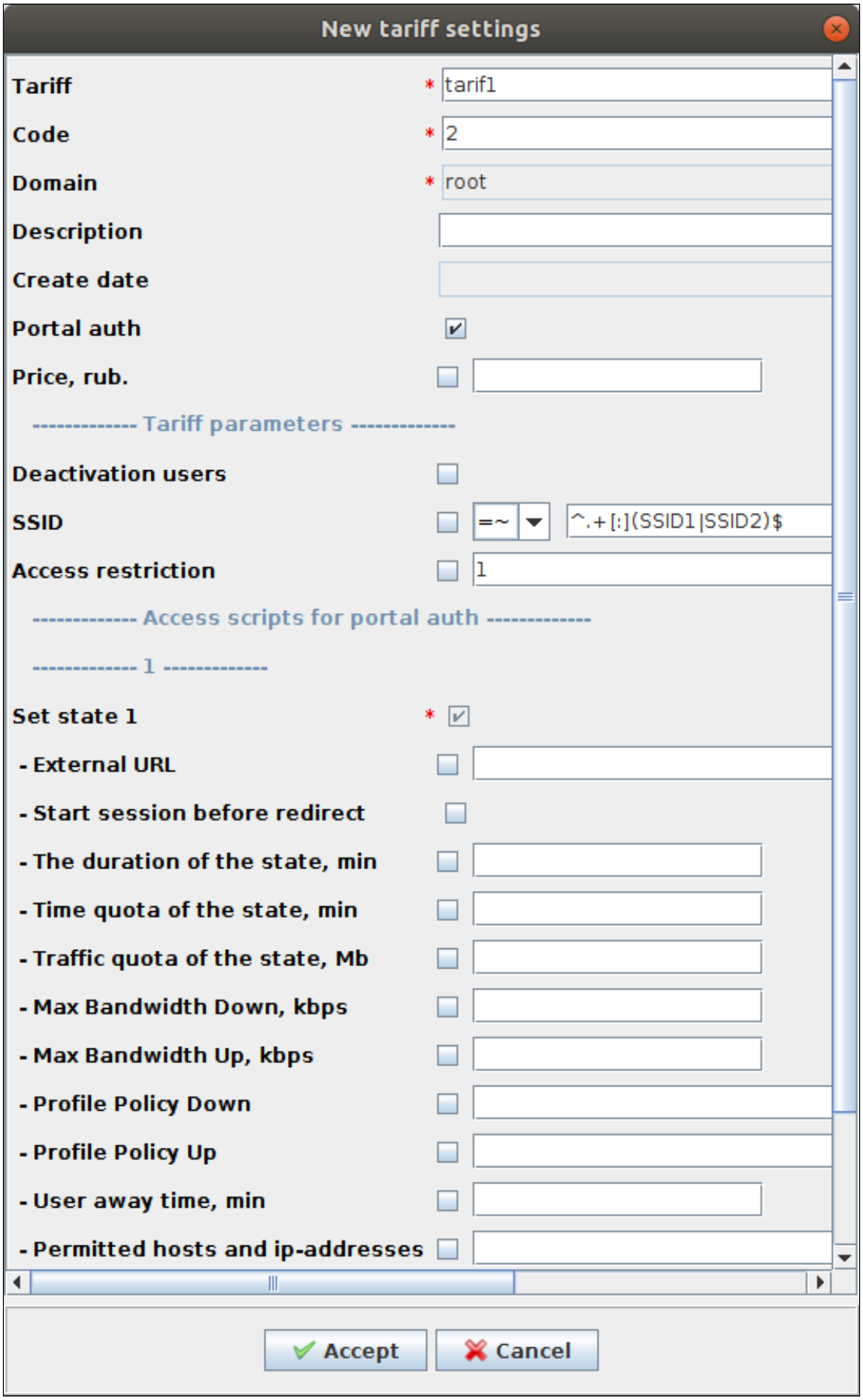

New tariff settings
Tariff
tarif1
Code
2
Domain
root
Description
Create date
Portal auth
Price, rub.
---------- Tariff parameters ----------
Deactivation users
SSID
=~
^.+[:](SSID1|SSID2)$
Access restriction
1
---------- Access scripts for portal auth ----------
---------- 1 ----------
Set state 1
- External URL
- Start session before redirect
- The duration of the state, min
- Time quota of the state, min
- Traffic quota of the state, Mb
- Max Bandwidth Down, kbps
- Max Bandwidth Up, kbps
- Profile Policy Down
- Profile Policy Up
- User away time, min
- Permitted hosts and ip-addresses
Accept
Cancel

*Figure 6 – New tariff settings*

5. Activate the tariff plan on the portal.
To activate, follow the link **192.168.50.1:8080/epadmin**.

**Login: admin**
**Password: password**

In the left panel, select the portal to which the redirection is configured in the created SSID (by default).
Read more about creating and customizing new portals in the section v1.14_Portal Constructor (EN)

Open **Tariff plans** tab, click **Add** button and set flag against the created tariff plan **tarif1**.

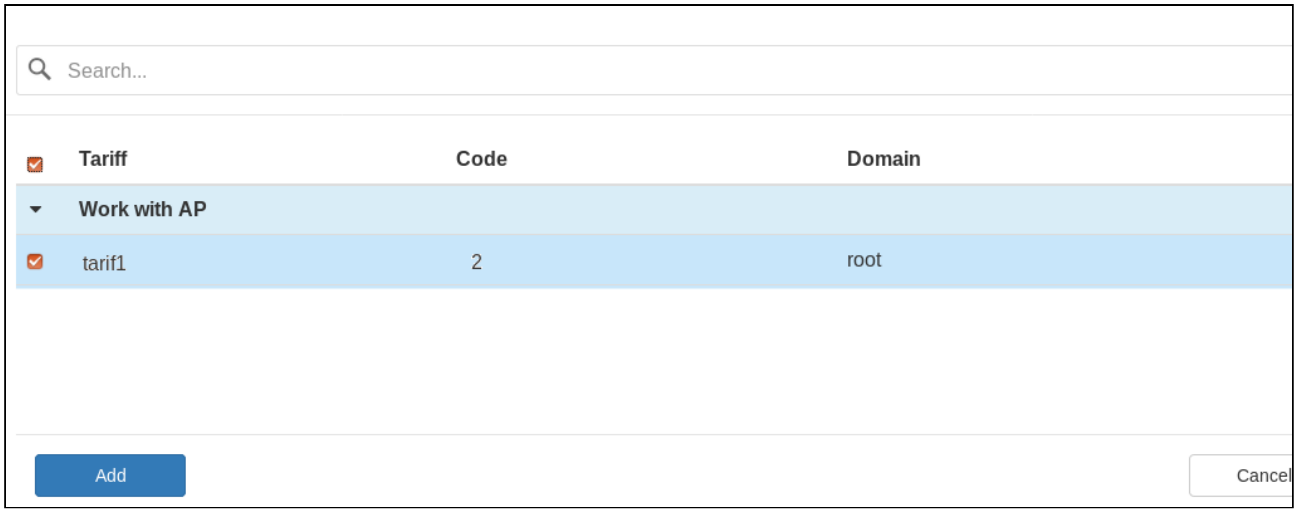



*Figure 7 – Selecting a tariff plan*

Enter its name which will be displayed to the client on the authorization page in case of using several tariff plans. Click **Save** button.

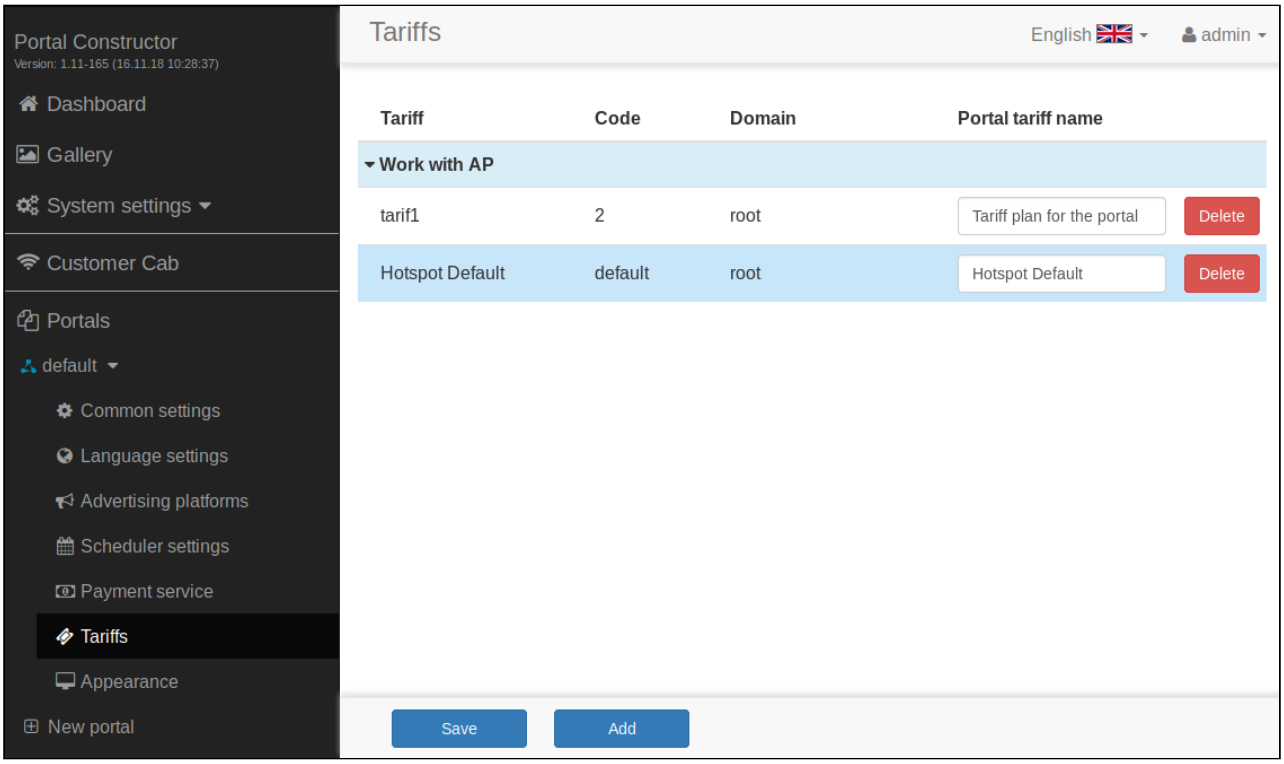
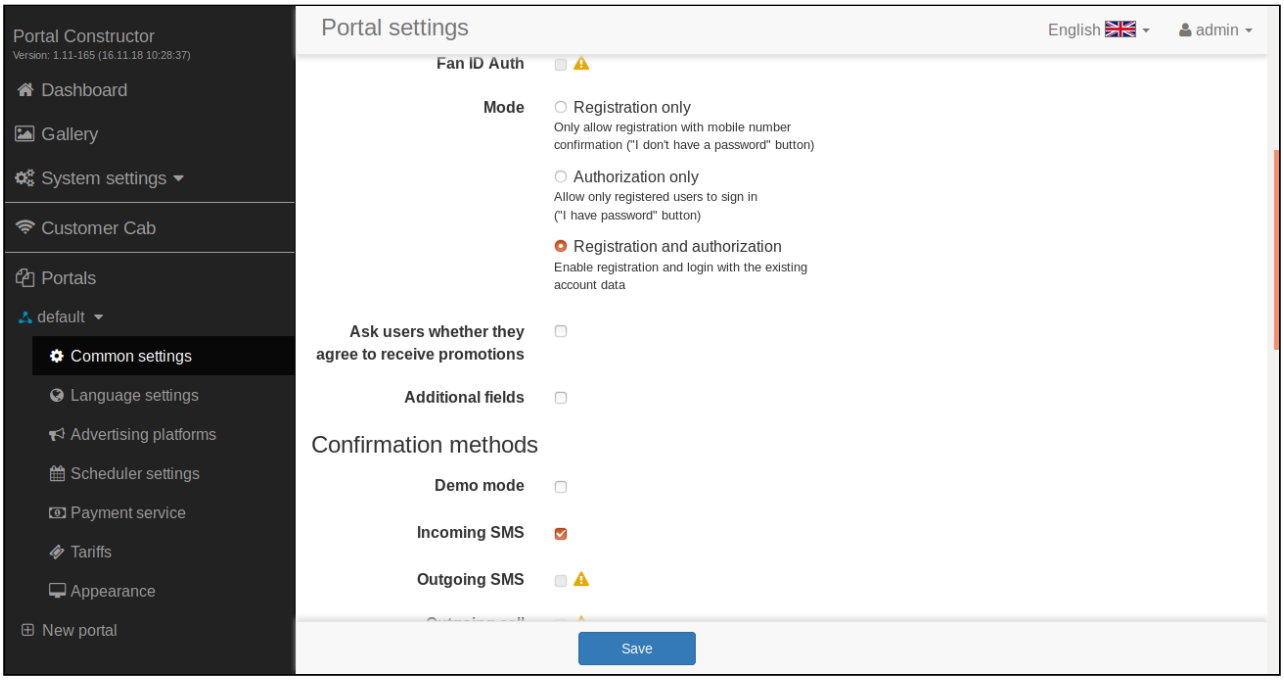



*Figure 8 – Activation of the tariff plan*

Portal operation modes and confirmation of phone numbers are configured in the menu "General settings" (see sections of the "Operation Mode" and "Confirm phone number" ). The **register and authorize** mode is used by default. To confirm the phone number in portal authorization, two ways are used: **Demo mode** и **Incoming SMS**. The demo mode is intended for testing, after entering the phone number, a code is generated and automatically inserted into the form. When putting the system into operation, deselect the **Demonstration Mode** check box.

Outgoing call and outgoing SMS confirmation methods become available for inclusion after they are configured in the configuration files.




Configure the **/etc/eltex-ngw/notification.properties** file for real SMG sending.

**Configuring the phone number confirmation by incoming messages when the** smsc.ru **gateway is used**

Depending on the interfacing protocol used, specify the required configuration file in the line of **sms.gate.outgoing.sms.config**:

- **smsc_gate.conf** for HTTP
- **smpp_gate.conf** for SMPP (v 3.4)

```
sms.gate.outgoing.sms.config=smsc_gate.conf
```

Contents of the **notification.properties** file:Use this file also for configuring message transmission.

```
#Common gates settings
#Current gate used for each type (config name, for example smpp_gate.conf)
sms.gate.outgoing.sms.config=smsc_gate.conf
#For incoming sms/calls fields for numbers in configs should be set
sms.gate.incoming.sms.config=
sms.gate.incoming.call.config=

#Gate pool settings
sms.gate.pool.size=50
sms.gate.pool.wait.millis=5000

#Port to listen for requests
server.port=8040

#============================
#=======database settings=====
#============================
#mongodb.uri=mongodb://192.168.1.1,192.168.1.2:27017/notification-gw
mongodb.host=localhost
mongodb.port=27017
#mongodb.user=user
#mongodb.password=password
mongodb.name=notification-gw
fsfiles.store.period=7

#============================
#=======email settings========
#============================
mail.smtp.submitter=test@email.com
mail.smtp.password=
mail.smtp.auth=true
mail.smtp.host=email.com
mail.smtp.port=587
mail.smtp.sendpartial=true
mail.smtp.starttls.enable=false
mail.smtp.connectiontimeout=5000
mail.gate.pool.size=20
mail.pool.wait.millis=10000

Next, edit the selected configuration file.
```

1. When using HTTP, it is **smsc_gate.conf**

Fill in **SMSC_LOGIN** and **SMSC_PASSWORD,** that are obtained on smsc.ru website**,** and **SMSC_PROTOCOL (http or https).**

Contents of the **smsc_gate.conf** file:

```
# SMSC settings

SMSC_USE_TRANSLIT=false
# smsc accounting (api) settings
SMSC_LOGIN=
# password for smsc account. If also using this account with smpp, password
should be no longer
# that 8 symbols according to specification of smpp protocol. Russian symbols
are not allowed
SMSC_PASSWORD=
# encoding for transferring sms via http protocol
SMSC_CHARSET=utf-8
SMSC_DEBUG=false
SMSC_USE_POST=false
# choosing protocol (http|https)
SMSC_PROTOCOL=http
SMSC_SENDER=
```

2. If SMPP is used, you should fill in the following data in the **smpp_gate.conf** configuration file: login, password, server address, port and other settings required to use SMPP.

Contents of **smpp_gate.conf** file:

```
# SMSC settings

SMSC_USE_TRANSLIT=false
# smsc accounting (api) settings
SMSC_LOGIN=
# password for smsc account. If also using this account with smpp, password
should be no longer
# that 8 symbols according to specification of smpp protocol. Russian symbols
are not allowed
SMSC_PASSWORD=
# encoding for transferring sms via http protocol
SMSC_CHARSET=utf-8
SMSC_DEBUG=false
SMSC_USE_POST=false
# choosing protocol (http|https)
SMSC_PROTOCOL=http
SMSC_SENDER=
vagrant@vagrant-ubuntu-trusty-64:~$ cat /etc/eltex-ngw/smpp_gate.conf
# SMPP Gate settings

# smsc accounting (api) settings
```

```
SMSC_LOGIN=
# password for smsc account. should be no longer than 8 symbols according
# to specification of smpp protocol. Russian symbols are not allowed
SMSC_PASSWORD=

# for enabling smpp via smsc.ru need to enable smpp-sending in smsc.ru
# private account settings and connect with smsc.ru support and tell them
# ip-address(es) from which connection(s) will be established and
# which port to open: regular or secured (ssl) (or both)

# host - name or IP
SMSC_SMPP_HOST=smpp.smsc.ru
SMSC_SMPP_PORT=3700
# reserved host for sending sms
SMSC_SMPP_RESERV_HOST=smpp2.smsc.ru
SMSC_SMPP_SSL_PORT=

# numbers for receiving incoming messages
# comma is a separator
NUMBERS_FOR_INCOMING_SMS=
# numbers for receiving incoming calls
# comma is a separator
NUMBERS_FOR_INCOMING_CALLS=

# seconds between sending ENQUIRE_LINK packet to maintain connection with
SMPP server
# for SMSC SMPP 15 seconds is OK
SMSC_SMPP_ENQUIRE_LINK_INTERVAL=15
# Seconds waiting response from SMPP server on SUBMIT_SM packet
SMSC_SMPP_TRANSACTION_INTERVAL=5
# type of number for ESME address - better use UNKNOWN (UNKNOWN|
INTERNATIONAL|
# NATIONAL|NETWORK_SPECIFIC|SUBSCRIBER_NUMBER|ALPHANUMERIC|ABBREVIATED)
SMSC_ESME_TYPE_OF_NUMBER=UNKNOWN
# numbering plan indicator for ESME address - better use UNKNOWN (UNKNOWN|
ISDN|
# DATA|TELEX|LAND_MOBILE|NATIONAL|PRIVATE|ERMES|INTERNET|WAP)
SMSC_ESME_NUMBERING_PLAN_INDICATOR=UNKNOWN
# service type - better leave empty for default (|CMT|CPT|VMN|VMA|WAP|USSD)
SMSC_SERVICE_TYPE=
# source address type of number when sending (UNKNOWN stands for 0|
INTERNATIONAL stands for 1|
# NATIONAL - 2|NETWORK_SPECIFIC - 3|SUBSCRIBER_NUMBER - 4|ALPHANUMERIC - 5|
ABBREVIATED - 6)
SMSC_SOURCE_ADDR_TYPE_OF_NUMBER=ALPHANUMERIC
# source address numbering plan indicator when sending (UNKNOWN stands for 0|
ISDN - 1|
# DATA - 2|TELEX - 3|LAND_MOBILE - 4|NATIONAL - 5|PRIVATE - 6|ERMES - 7|
```

```
INTERNET - 8|WAP - 9)
SMSC_SOURCE_ADDR_NUMBERING_PLAN_INDICATOR=ISDN
# source address to indicate in smsc.ru log, can give any name or leave
empty, max length is 20 symbols
# russian symbols will be converted to translit
SMSC_SOURCE_ADDRESS=
# destination address type of number when sending (UNKNOWN stands for 0|
INTERNATIONAL - 1|NATIONAL - 2|
# NETWORK_SPECIFIC - 3|SUBSCRIBER_NUMBER - 4|ALPHANUMERIC - 5|ABBREVIATED -
6)
SMSC_DEST_ADDR_TYPE_OF_NUMBER=INTERNATIONAL
# destination address numbering plan indicator when sending (UNKNOWN stands
for 0|ISDN - 1|DATA - 2|
# TELEX - 3|LAND_MOBILE - 4|NATIONAL - 5|PRIVATE - 6|ERMES - 7|INTERNET - 8|
WAP - 9)
SMSC_DEST_ADDR_NUMBERING_PLAN_INDICATOR=ISDN
# replace message prefix with another one or nothing
SMSC_DEST_ADDR_REPLACE_PREFIX=
SMSC_DEST_ADDR_REPLACE_PREFIX_WITH=
# protocol ID
SMSC_PROTOCOL_ID=0
# flag shows priority of sms in smsc queue (0|1|2|3) 3 - the highest
SMSC_PRIORITY_FLAG=3
# encoding (1 stands for 8-bit ASCII|2 for UCS2 (UTF-16)|0 for 7-bit in data
coding, but for text will be used UTF-8).
# For sending messages with cyrillic text use 2
SMSC_ENCODING=2
# encode text in win1251, but send data coding marker as defined above
SMSC_ENCODE_WIN1251=FALSE
# concat long text on smpp server into 1 message (TRUE|FALSE). May pay less
money of concatting
SMSC_CONCAT_LONG_TEXT_ON_SMPP_SERVER=TRUE
# ESME settings
# MessageMode (DEFAULT stands for 0|DATAGRAM - 1|TRANSACTION - 2|
STORE_AND_FORWARD - 3)
SMSC_MESSAGE_MODE=DATAGRAM
# MessageType (DEFAULT|ESME_DEL_ACK|ESME_MAN_ACK|SMSC_DEL_RECEIPT|
SME_DEL_ACK|SME_MAN_ACK|CONV_ABORT|INTER_DEL_NOTIF)
SMSC_MESSAGE_TYPE=DEFAULT
# GSMSpecificFeature (DEFAULT|UDHI|REPLYPATH|UDHI_REPLYPATH)
SMSC_GSM_SPECIFIC_FEATURE=DEFAULT
# GeneralDataCoding settings
# ignore these settings (for proper data coding 0x08, for ex.) (TRUE|FALSE)
SMSC_IGNORE_OPTIONAL_DATA_CODING_SETTINGS=TRUE
# compressed (FALSE|TRUE)
SMSC_COMPRESSED=FALSE
# messageClass (0|1|2|3)
SMSC_MESSAGE_CLASS=1
```

Save the settings and restart the service by using command:

```
sudo service eltex-ngw restart
```

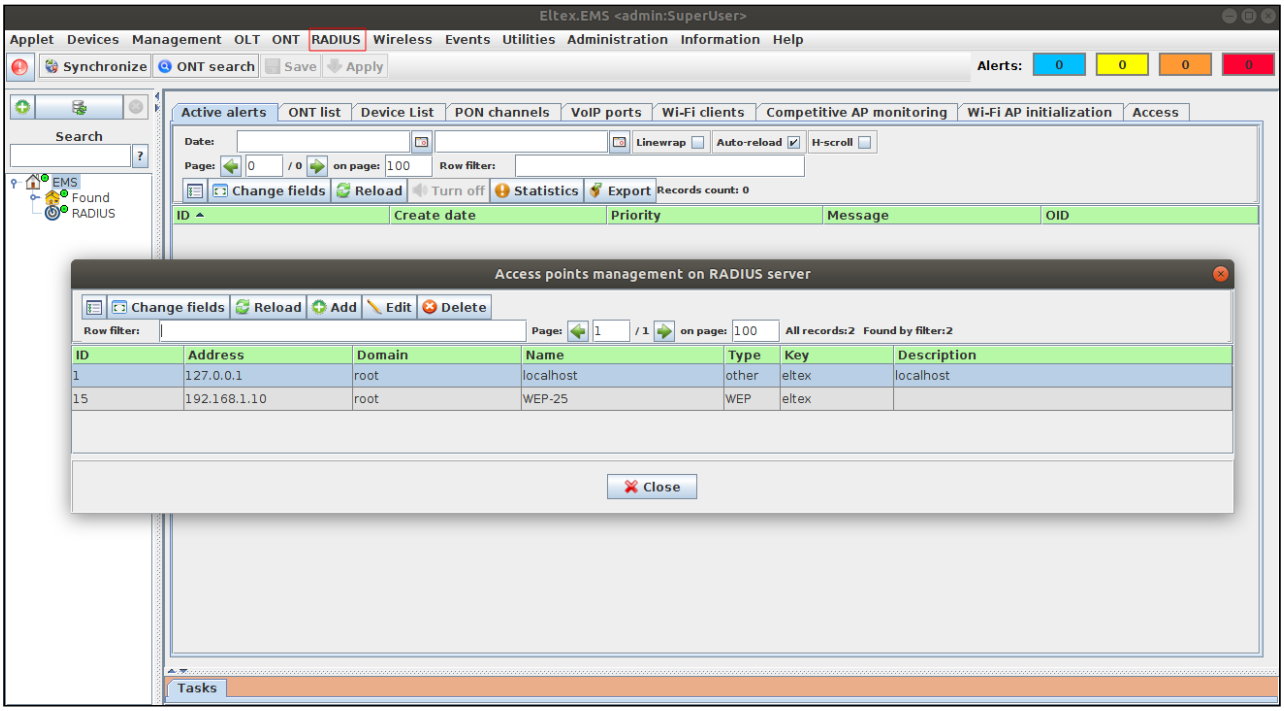
[1] There is a "default" page on the portal by default. The page is customized for ELTEX Company as an example.

[2] The name of the group within which roaming can be carried out in case of portal authorization. If the access point has a firmware 1.9.0, you should specify **user mobility domain**. This option is not available in firmware versions above 1.9.0.

## v1.14_Quickstart for configuring a Wi-Fi Enterprise network

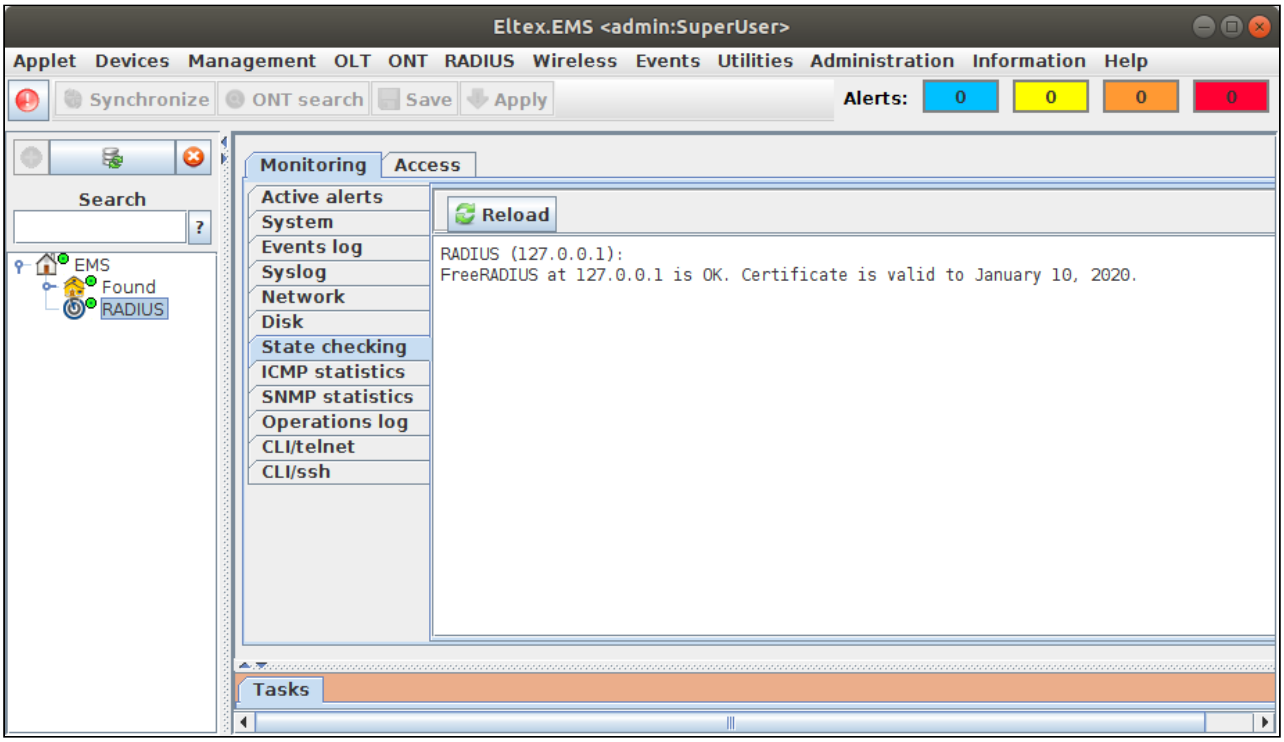
### 1. Checking for an access point (AP) in the Radius database

Before configuring the AP, you should verify that it is added to the NAS table of the Radius server. To do this, open the **RADIUS/Access points management on RADIUS server** menu. Find the access point by using the IP address filter.




### 2. RADIUS status checking

Select the RADIUS object in the object tree and go to the **Monitoring/State checking** menu.

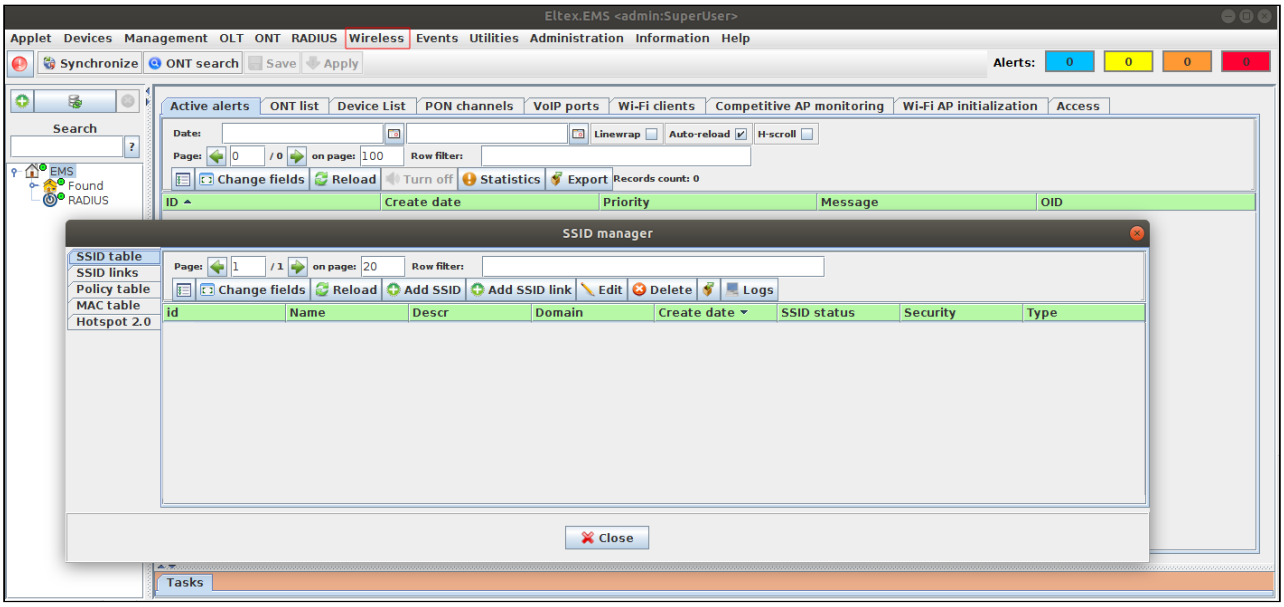



Connect to the server console and start the command to verify that the process is running:

```
root@SoftWLC:/home/tester# ps -aux | grep eltex-radius
eltxrad   1609  0.0  0.9 358824 19728 ?        Ssl  10:29   0:00 /usr/sbin/
eltex-radius -f
root      6563  0.0  0.1  11688  2176 pts/0    S+   12:49   0:00 grep --
color=auto eltex-radius
```

### 3. SSID configuration

Open the SSID Manager in the **Wireless/SSID manager** menu.




Click **Add SSID** .

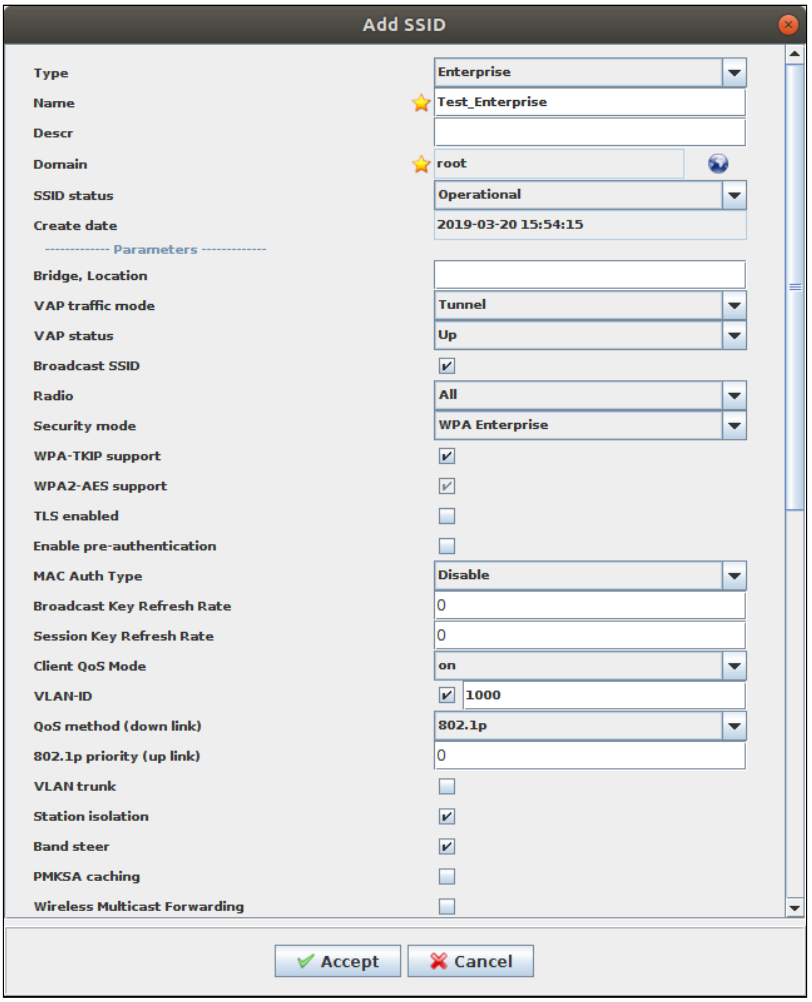
Set the following key settings:

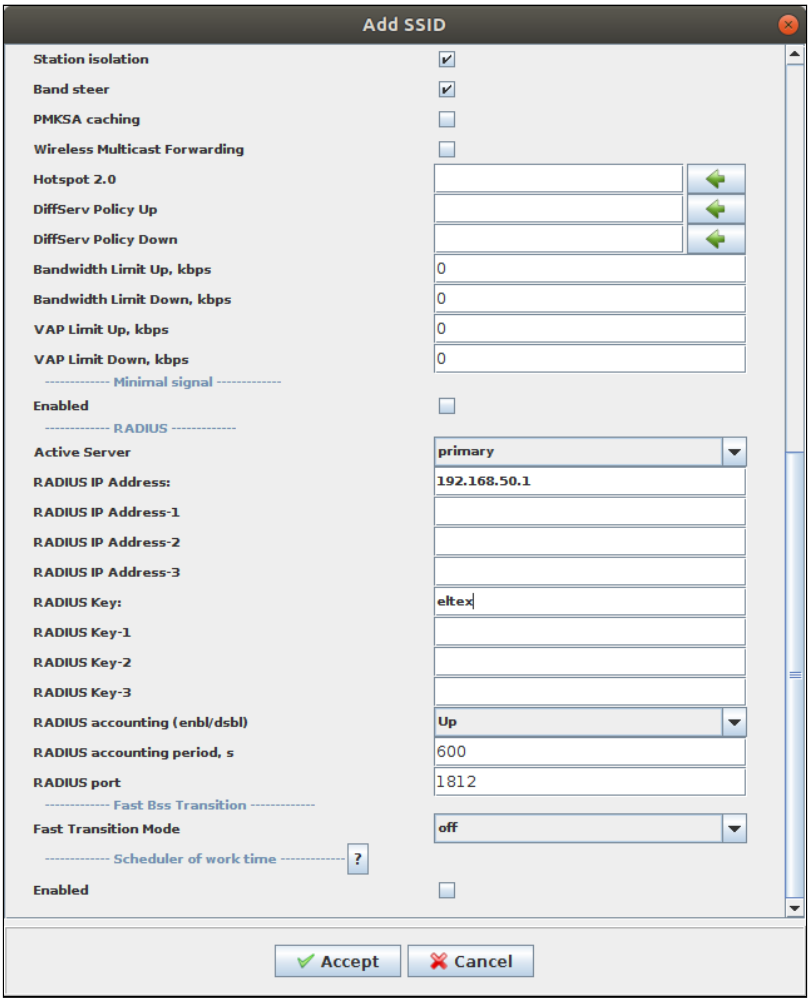
```
Type – Enterprise
Name – Test_enterprise
Domain – root
Security mode – WPA Enterprise
RADIUS IP Address – 192.168.50.1 (ip address of Your Radius server).
RADIUS Key – eltex
RADIUS accounting – up
RADIUS accounting period – 600
```

Select the Radio interfaces to which the generated SSID will be assigned.

When you assign a SSID to all radio interfaces simultaneously ("Radio" - "All"), it is recommended to enable **Band steer** (select check box) for priority connection to the 5 GHz network by devices that support both bands.

When you assign a SSID on one radio interface, the **Band steer** mode should be off.

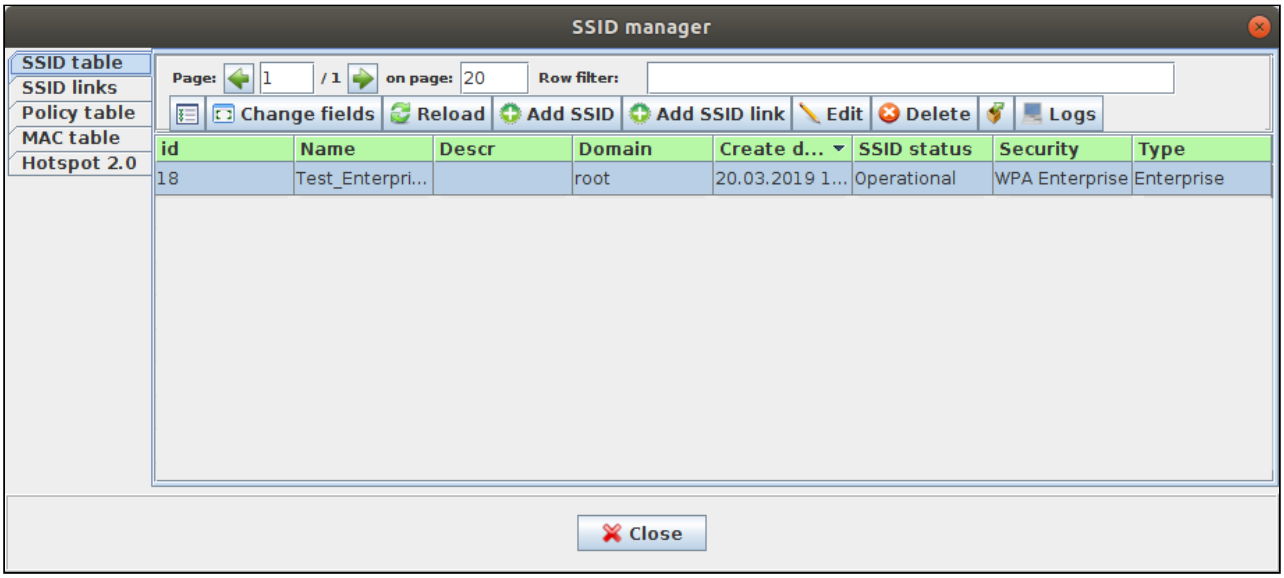

Add SSID
Type
Enterprise
Name
Test_Enterprise
Descr
Domain
root
SSID status
Operational
Create date
2019-03-20 15:54:15
---------- Parameters ----------
Bridge, Location
VAP traffic mode
Tunnel
VAP status
Up
Broadcast SSID
Radio
All
Security mode
WPA Enterprise
WPA-TKIP support
WPA2-AES support
TLS enabled
Enable pre-authentication
MAC Auth Type
Disable
Broadcast Key Refresh Rate
0
Session Key Refresh Rate
0
Client QoS Mode
on
VLAN-ID
1000
QoS method (down link)
802.1p
802.1p priority (up link)
0
VLAN trunk
Station isolation
Band steer
PMKSA caching
Wireless Multicast Forwarding
Accept
Cancel



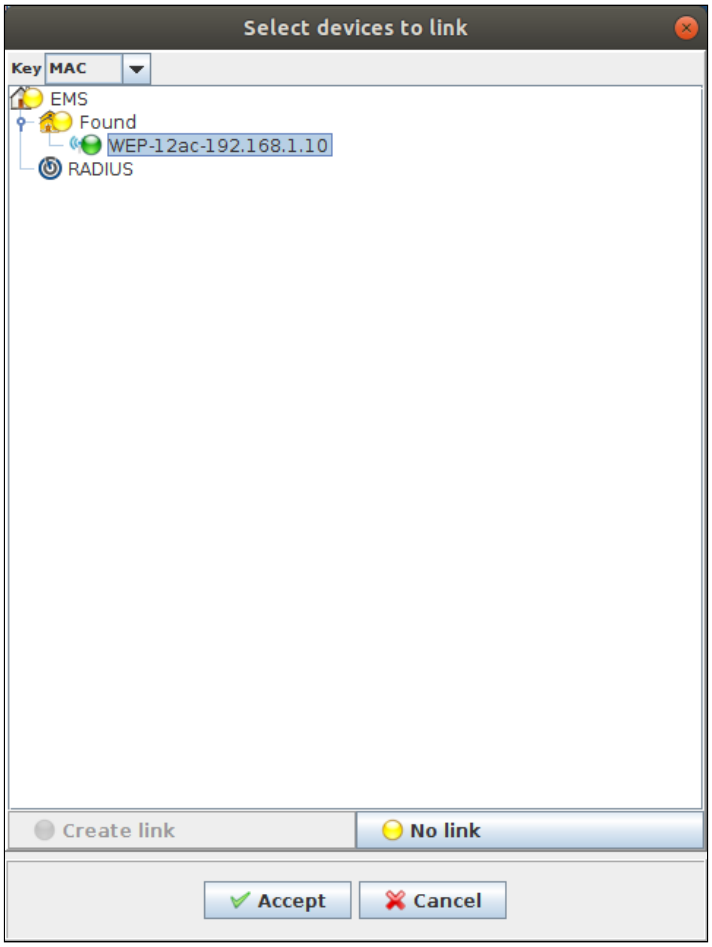

**Примечание**

VLAN-ID = 1000 is used as an example. It should be specified here the service VLAN that is actually used on Your network and comes to the access point. The DHCP server must be available to users in the VLAN.

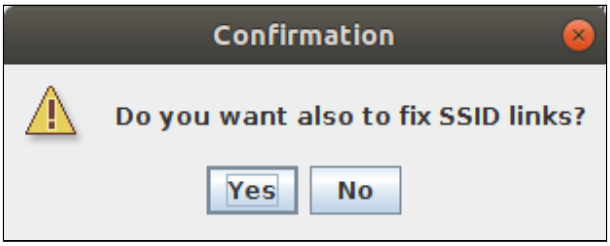
After clicking the **Accept** button, the SSID created will be displayed in the **SSID table**.



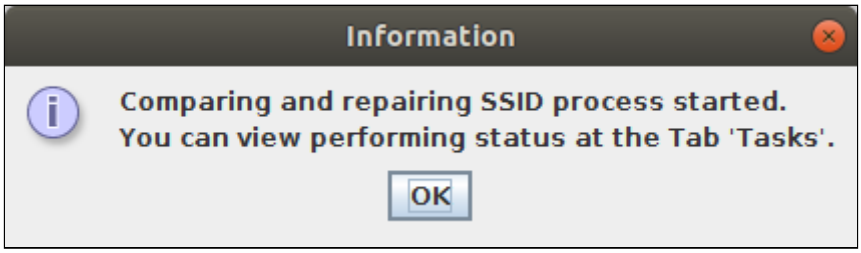

Assign SSID to the access point. To do that, select created SSID and click **Add SSID link** button. In the appeared window, select the key for binding. Binding can be performed by MAC address or IP address of AP or by the host domain. Binding can be performed by MAC address of AP, by IP address of AP, or by the host domain. Then select the objects to bind (access points or nodes) and click **Create binding**, the indicator in the tree will change from yellow to green. Click **Accept** button.



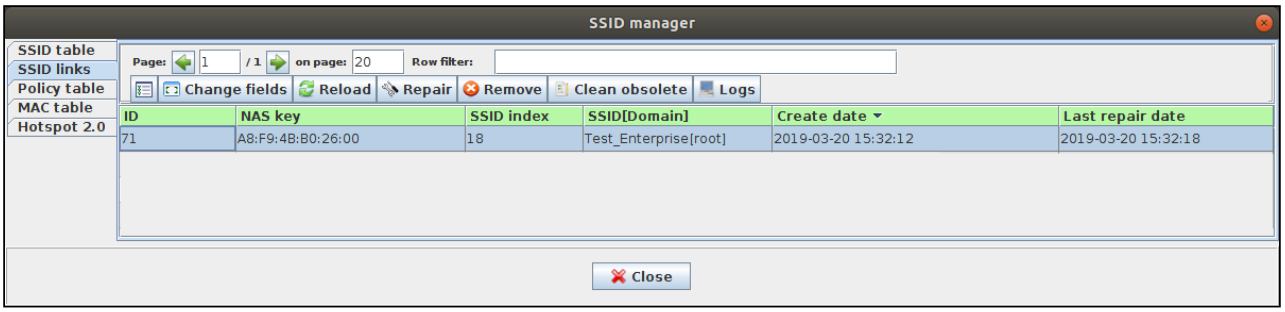

A window will appear with the question “Do you want to fix SSID bindings?”. If you want to assign the created SSID to the points immediately, select “yes”. If it is necessary that the binding exists only in the database, but does not apply now to the access point - click “No”. Then, if necessary, you can go to the “SSID Bindings” tab and click the “Fix” button to assign SSID to the access point, or the binding will be corrected by triggering the corresponding monitor (default once a day).



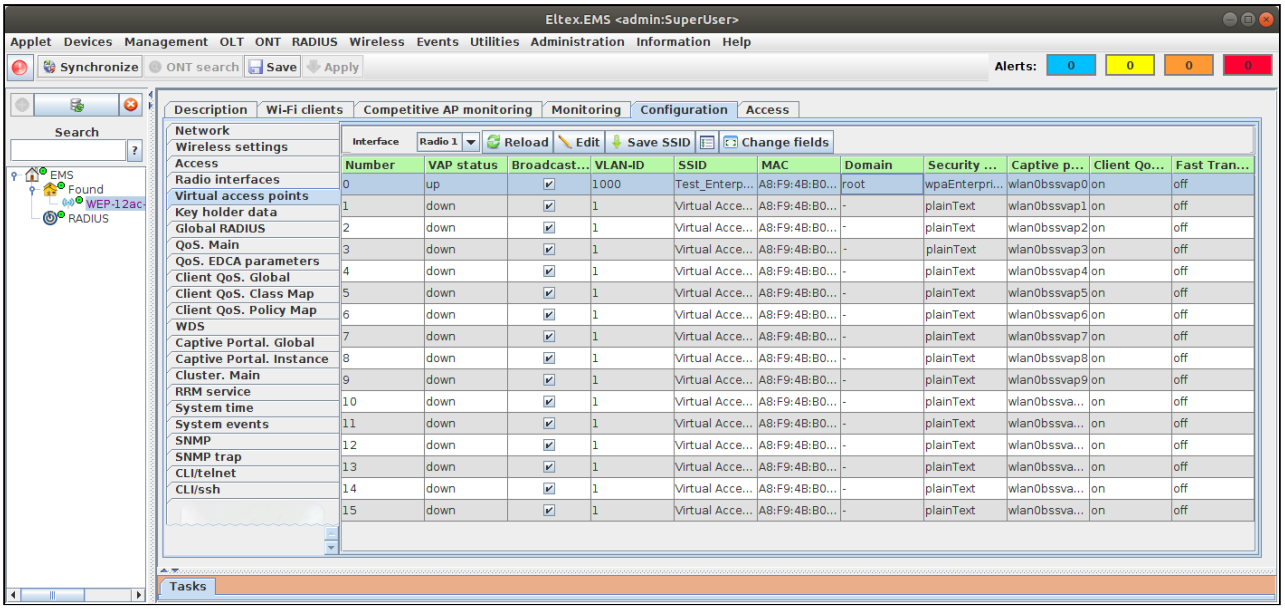

You can control the SSID assignment process in the **Tasks** tab.




The created binding appears in the **SSID links** tab .




The SSID will be assigned to the first disabled VAP on the access point. You can see the result in the **Configuration/Virtual access points** tab.




### 4. Creating Wi-Fi user accounts

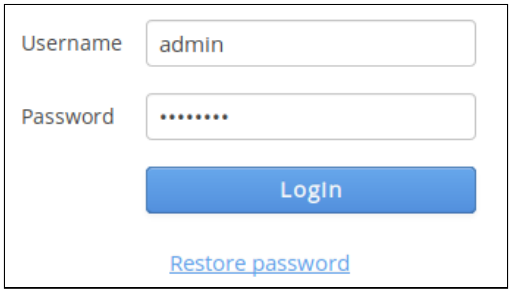
The creation of accounts is performed in your Personal account.

To do this, go to the browser link:

```
http://192.168.50.1:8080/wifi-cab/
```

In the window that opens, enter the administrator credentials:

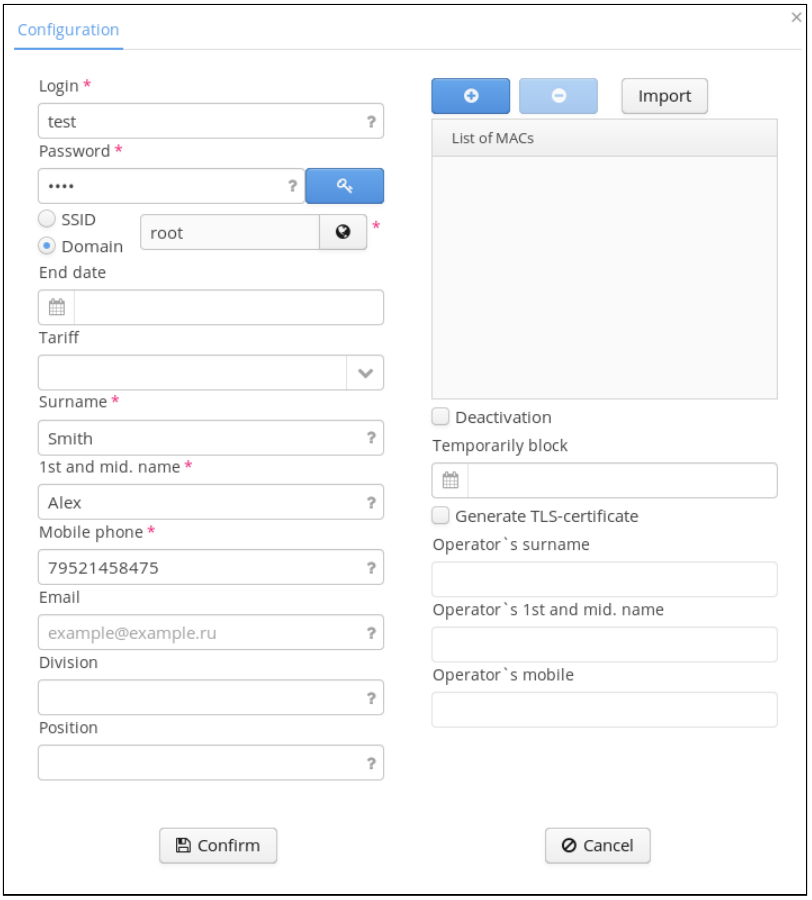
```
User name: admin
Password: password
```



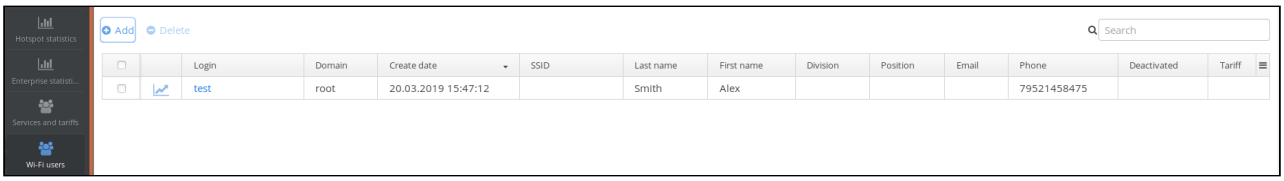

Go to the **Wi-Fi Users/Enterprise Users** tab.

Click the **Add** button.

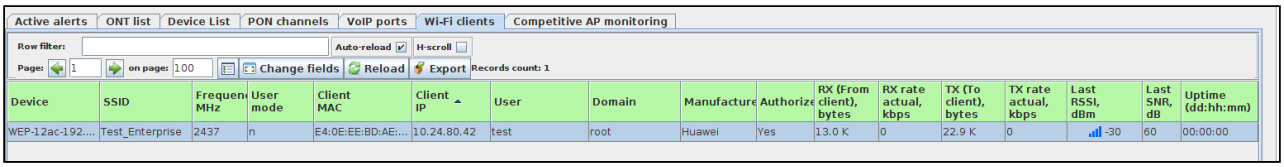
Set the login and password for the user, for example *test/test*. If necessary, the password can be generated by clicking the corresponding button at the end of the line  .



If the SSID flag is set, authorization of this user will be possible only on the selected SSID.
If the Domain flag is set, authorization of the user will be possible on any SSID belonging to the selected domain.
If it is required, specify additional parameters: account validity time, tariff (previously created with specified restrictions), user name, mobile phone/Email, where new authorization data will be sent when changing them on schedule.
Click the **Confirm** button.
The user appears in the table.




Data about connected users will be displayed in EMS in the **Wi-Fi Clients** tab.




## v1.14_SoftWLC installation and update (EN)


- v1.14_Step-by-step SoftWLC installation guide (the example for v1.7)
- v1.14_Step-by-step SoftWLC installation using the installation script
- v1.14_Recommendations after installation of SoftWLC
- v1.14_SoftWLC multihost system installation


## v1.14_Step-by-step SoftWLC installation guide (the example for v1.7)


- Preparing for installation
- Installation
  - Adding Eltex repositories
  - Adding third-party repositories
  - Adding a digital signature
  - Searching and installing package updates
  - Specifying root user's password for mysql database
  - Installing mysql-server
  - Confirming the agreement with the license before installing Oracle Java 8
  - Installing Oracle Java 8
  - Installing optional packages

    - Specifying JAVA_HOME environmental variable for tomcat7
    - Setting a timezone
    - Allocating extra memory for Java
    - Installing the eltex-notification-gw package
    - Installing the eltex-apb package
    - Installing the framework for SOAP/XML (Apache Axis) service
    - Installing the eltex-radius-nbi package to establish communication between SoftWLC and higher OSS/BSS
    - Installing the RADIUS service modified framework to MySQL
    - Installing the Auth Service database
    - Installing SoftWLC Authentication and authorization service
    - Installing the package to translate MAC addresses to vendors' names
    - Installing the eltex-radius package
    - Installing the Portal database
    - Installing Portal Constructor for customization
    - Installing the portal for Hotspot authorization of Wi-Fi clients
    - Installing the RADIUS service framework to MySQL
    - Installing the eltex-ems package
    - Installing B2B Admin Panel and management interface
- Installing the license for Eltex EMS


License Details

Invalid commercial evaluation license with a expired error

## Preparing for installation

To install SoftWLC minimum configuration, the server with the following parameters is required:

- Random access memory size >= 8 GB
- CPU >= 2200MHz
- Hard drive capacity >= 35 GB
- Internet connection
- Ubuntu 16.04 operating system

Find more information on server requirements here
Checking random access memory:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant free -m
 total used free shared buffers cached
Mem: 7985 409 7575 0 12 228
-/+ buffers/cache: 168 7816
Swap: 0 0 0
```

Checking CPU:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
CPU(s): 2
On-line CPU(s) list: 0,1
Thread(s) per core: 1
Core(s) per socket: 2
Socket(s): 1
NUMA node(s): 1
Vendor ID: GenuineIntel
CPU family: 6
Model: 60
Stepping: 3
CPU MHz: 3294.301
BogoMIPS: 6588.60
L1d cache: 32K
L1d cache: 32K
L2d cache: 6144K
NUMA node0 CPU(s): 0,1
```

Checking hard drive capacity:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# df -h
Filesystem Size Used Avail Use% Mounted on
udev 3.9G 12K 3.9G 1% /dev
tmpfs 799M 436K 799M 1% /run
/dev/sda1 40G 1.4G 37G 4% /
none 4.0K 0 4.0K 0% /sys/fs/cgroup
none 5.0M 0 5.0M 0% /run/lock
none 3.9G 0 3.9G 0% /run/shm
none 100M 0 100M 0% /run/user
none 901G 113G 789G 13% /vagrant
```

Checking a version of the operating system:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.6 LTS"
```

Checking Internet connection:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ping eltex.nsk.ru
PING eltex.nsk.ru (62.109.0.175) 56(84) bytes of data.
64 bytes from mail.eltex.nsk.ru (62.109.0.175): icmp_seq=1 ttl=55 time=52.8 ms
64 bytes from mail.eltex.nsk.ru (62.109.0.175): icmp_seq=2 ttl=55 time=47.6 ms
64 bytes from mail.eltex.nsk.ru (62.109.0.175): icmp_seq=3 ttl=55 time=46.4 ms
64 bytes from mail.eltex.nsk.ru (62.109.0.175): icmp_seq=4 ttl=55 time=46.5 ms
64 bytes from mail.eltex.nsk.ru (62.109.0.175): icmp_seq=5 ttl=55 time=46.3 ms
^C
--- eltex.nsk.ru ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 46.398/47.977/52.889/2.516 ms
```

## Installation

Adding Eltex repositories

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "deb http://
archive.eltex.org/ems 3.12 main" >> /etc/apt/sources.list.d/eltex.list
```

Adding third-party repositories

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# add-apt-repository -y
ppa:webupd8team/java
gpg: keyring `/tmp/tmpvow23jgr/secring.gpg' created
gpg: keyring `/tmp/tmpvow23jgr/pubring.gpg' created
gpg: requesting key EEA14886 from hkp server keyserver.ubuntu.com
gpg: /tmp/tmpvow23jgr/trustdb.gpg: trustdb created
gpg: key EEA14886: public key "Launchpad VLC" imported
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
OK
```

Adding a digital signature

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-key adv --keyserver
keyserver.ubuntu.com --recv F558A287
Executing: gpg --ignore-time-conflict --no-options --no-default-keyring --
homedir /tmp/tmp.JjIxiUgI0p --no-auto-check-trustdb --trust-model always --
keyring /etc/apt/trusted.gpg --primary-keyring /etc/apt/trusted.gpg --
keyring /etc/apt/trusted.gpg.d/webupd8team-java.gpg --keyserver
keyserver.ubuntu.com --recv F558A287
gpg: requesting key F558A287 from hkp server keyserver.ubuntu.com
gpg: key F558A287: public key "Eltex.EMS build server (Signing for inner Eltex
debian packages) <aleksey.sergeev@eltex.nsk.ru>" imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

Searching and installing package updates

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get update
...
Fetched 12.1 MB in 19s (624 kB/s)
Reading package lists... Done
```

Specifying root user's password for mysql database

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# debconf-set-selections <<<
'mysql-server mysql-server/root_password password root'
root@vagrant-ubuntu-trusty-64:/home/vagrant# debconf-set-selections <<<
'mysql-server mysql-server/root_password_again password root'
```

Installing mysql-server

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get -y install mysql-server
```

Confirming the agreement with the license before installing Oracle Java 8

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo debconf shared/accepted-
oracle-license-v1-1 select true | sudo debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo debconf shared/accepted-
oracle-license-v1-1 seen true | sudo debconf-set-selections
```

Installing Oracle Java 8

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get -y install oracle-java8-
installer
```

Installing optional packages

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/dbconfig-install boolean true" | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/mysql/app-pass password root" | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/app-password-confirm password root" | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/password-confirm password root" | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/mysql/admin-pass password root" | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "rsyslog-mysql rsyslog-
mysql/remote/port string " | debconf-set-selections
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install --yes expect
daemon psmisc mysql-client ntp tftp-hpa tftpd-hpa snmpd snmp rsyslog rsyslog-
mysql curl tomcat7 software-properties-common python-pexpect unzip zip
mongodb-server isc-dhcp-server pcscd opensc pcsc-tools pkiclient libhal1
python-suds libtalloc2 libwbclient0 tomcat7-admin
```

Specifying JAVA_HOME environmental variable for tomcat7

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "JAVA_HOME=/usr/lib/jvm/
java-8-oracle" >> /etc/default/tomcat7
```

Setting a timezone

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# cp /usr/share/zoneinfo/Asia/
Novosibirsk /etc/localtime
```

Allocating extra memory for Java

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "JAVA_OPTS=\"${JAVA_OPTS}
-server -Xms512m -Xmx2048m -XX:-UseParallelGC -XX:+UseConcMarkSweepGC -XX:
+AggressiveOpts\"" >> /etc/default/tomcat7
```

Installing the eltex-notification-gw package

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

Installing the eltex-apb package

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

Installing the framework for SOAP/XML (Apache Axis) service

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

Installing the eltex-radius-nbi package to establish communication between SoftWLC and higher OSS/BSS

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-radius-nbi
...
Do you want to generate server certificate? [y/N]: N
Skip generating server certificate
- Reconfigure file '/etc/eltex-radius-nbi/radius_nbi_config.txt'
SoftWLC Northbound is installed. Tomcat service will be restarted...
 * Stopping Tomcat servlet engine tomcat6
 ...done.
 * Starting Tomcat servlet engine tomcat6
 ...done.
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/
```

Installing the RADIUS service modified framework to MySQL

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-radius-db
...
Enter your MySQL administrator login (default is 'root'): root
Enter your MySQL administrator password: root
Enable remote access to database? (y/N) y
mysql stop/waiting
mysql start/running, process 17341
Creating database ...
Preparing database ...
Do you want to create a tariff? (Y/n) Y
Enter root domain name (default is 'root'): root
Enter tariff code (its identifier) (default is 'default'): 1
Tariff '1' has been successfully created
There are two types of tariffs:
 * Tariff for hotspot with captive portal authorization
 * Tariff for customers with WPA Enterprise authorization
Make the tariff for portal authentication only? (Y/n) Y
Please restart RADIUS server manually with "service eltex-radius restart"
```

After the installation has finished, the "Hotspot Default" tariff plan will be created in the system to carry out portal authorization with the following parameters:

- Tariff code: default
- Domain: root
- Portal authentication checkbox is set
- Duration: 10 minutes
- Downstream and Upstream speed limit is 1 Mbps

The tariff is referenced to the Default portal in Portal Constructor

Installing the Auth Service database

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-auth-
service-db
...
Enter your mysql administrator login (default is 'root'): root
Enter your mysql administrator password: root
Creating database 'eltex_auth_service'
Create remote database user? (y/N) y
Database 'eltex_auth_service' successfully created
Restart the service with command "service eltex-auth-service restart"
Enter root domain [root]: root
Create default auth-user:
Set login [admin]:
Set password [password]:
Default auth-user 'admin' created successfully
Set service user password [softwlc]:
Service user 'softwlc_service' created successfully. Please, check it at '/
etc/eltex-wifi-cab/system.xml' on your 'Eltex Wi-Fi customer cabinet' host.
Create default auth-nas (for eltex-wifi-cab):
Set eltex-wifi-cab ip address (leave empty if 127.0.0.1):
Default auth-nas '127.0.0.1' created successfully
```

Installing SoftWLC Authentication and authorization service

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

Installing the package to translate MAC addresses to vendors' names

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

Installing the eltex-radius package

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

Installing the Portal database

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-portal-
mysql
...
Enter your MySQL administrator login (default is 'root'): root
Enter your MySQL administrator password: root
Creating main database 'ELTEX_PORTAL'
```

Installing Portal Constructor for customization

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

Installing the portal for Hotspot authorization of Wi-Fi clients

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

Installing the RADIUS service framework to MySQL

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-ems-db
...
Enter your MySQL administrator password: root
Enable remote access to database? (y/N) y
...
Select default language for EMS:
 1. Russian
 2. English (default)
Enter number: 1
Using locale ru_RU
Select access control type:
 1 - Role based
 2 - Domain based (default)
Enter number: 2
Using domain based access control
Enter root domain name (default is 'root'):
Please restart EMS manually with "service eltex-ems restart"
```

Installing the eltex-ems package

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-ems
...
Replace /etc/default/tftpd-hpa? (type 'd' to view diff) [y/N/d] y
File /etc/default/tftpd-hpa is overwritten
Restarting tftpd-hpa..
tftpd-hpa stop/waiting
tftpd-hpa start/running, process 19261
Replace /etc/snmp/snmpd.conf? (type 'd' to view diff) [y/N/d] y
File /etc/snmp/snmpd.conf is overwritten
Restarting snmpd..
 * Restarting network management services:
Replace /etc/rsyslog.conf? (type 'd' to view diff) [y/N/d] y
File /etc/rsyslog.conf is overwritten
Replace /etc/rsyslog.d/50-default.conf? (type 'd' to view diff) [y/N/d] y
File /etc/rsyslog.d/50-default.conf is overwritten
Replace /etc/rsyslog.d/mysql.conf? (type 'd' to view diff) [y/N/d] y
File /etc/rsyslog.d/mysql.conf is overwritten
```

Installing B2B Admin Panel and management interface

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

## Installing the license for Eltex EMS

ⓘ The license file for Eltex EMS license.xml package contains information on the number and type of EMS-compatible devices. The file is provided by Commercial Department of Eltex Company or its partners.

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# cp licence.xml /usr/lib/eltex-ems/conf/licence/
root@vagrant-ubuntu-trusty-64:/home/vagrant# service eltex-ems restart
```

# v1.14_Step-by-step SoftWLC installation using the installation script

## Preparing for installation

To install a minimum configuration of SoftWLC, the server with the following parameters is required:

- Random access memory size >= 8 GB
- CPU >= 2200MHz
- Hard drive capacity >= 35 GB
- Internet connection
- Ubuntu 16.04 operating system

Find more information on server requirements here.
It is recommended to clean install the controller.

## Installation

Download the archive with the relevant eltex-softwlc-helper-mos_1.XX.sh installation script and save it to the root directory of the operating system.

The operation can also be performed via the terminal:

```
vagrant@ubuntu-xenial:~$ wget http://archive.eltex.org/wireless/help/softwlc-1.14/eltex-softwlc-helper-mos_1.14.sh

--2019-07-18 11:28:43-- http://archive.eltex.org/wireless/help/softwlc-1.14/eltex-softwlc-helper-mos_1.14.sh
Resolving archive.eltex.org (archive.eltex.org)… 172.16.5.22
Connecting to archive.eltex.org  (archive.eltex.org)|172.16.5.22|:80... connected.
HTTP request sent. Awaiting response... 200 OK
Length: 25961 (25K) [text/x-sh]
Saving to: «eltex-softwlc-helper-mos_1.14.sh»

eltex-softwlc-helper-mos_1.14.sh 100%
[=======================================================================>]
25,35K --.-KB/s за 0s

2019-07-18 11:28:43 (102 MB/s) - «eltex-softwlc-helper-mos_1.14.sh» saved [25961/25961]
```

Assign permission to execute the eltex-softwlc-helper-mos_1.14.sh file:

```
vagrant@ubuntu-xenial:~$ chmod +x ./eltex-softwlc-helper-mos_1.14.sh
```

Start the script under the super user and wait for the completion:

```
vagrant@ubuntu-xenial:~$ sudo ./eltex-softwlc-helper-mos_1.14.sh
Platform : x86_64
Repository: http://archive.eltex-co.ru/wireless
Java vendor: openjdk
Ubuntu distrib code name: xenial
--2019-04-29 08:33:06-- http://archive.eltex-co.ru/wireless/nginx/conf/softwlc_1.XX_nginx.conf
Resolving archive.eltex-co.ru (archive.eltex-co.ru)... 172.16.0.68
Connecting to archive.eltex-co.ru (archive.eltex-co.ru)|172.16.0.68|:80... connected.
HTTP request sent, awaiting response... 200 OK

. . . . . .
```

Upon completion of the work, the following data will be available in the terminal:

```
Installation of Eltex SoftWLC finished
URLs of SoftWLC components:
Eltex.EMS GUI: http://localhost:8080/ems/jws
login: admin
password: <empty>

Portal constructor: http://localhost:8080/epadmin
login: admin
password: password

Wi-Fi customer cabinet: http://localhost:8080/wifi-cab
login: admin
password: password
```

The script installs software using default passwords. If custom passwords are necessary, edit them before installation and save the script.

```
# MySQL administrator's username
export ANSWER_SOFTWLC_MYSQL_USER=root
# MySQL administrator's password
export ANSWER_SOFTWLC_MYSQL_PASSWORD=root
# SoftWLC administrator's username
export ANSWER_AUTH_SERVICE_ADMIN_USER=admin
# SoftWLC administrator's password
export ANSWER_AUTH_SERVICE_ADMIN_PASSWORD=password
# SoftWLC service user's password (softwlc_service)
export ANSWER_SOFTWLC_SERVICE_USER_PASSWORD=softwlc
```

After changing the password, duplicate the changes in SoftWLC modules:

v1.14_How to change a password for accessing Admin Panel_Portal Constructor (EN)

## v1.14_Recommendations after installation of SoftWLC

A library used in JVM Oracle for random number generation applies */dev/random* for UNIX platforms by default. This can lead to slow download speed of the WebLogic Server process.
It is recommended to use */dev/urandom*, if the default JVM configuration starts the WebLogic server too slowly. To determine if any problems occur when starting the server, enter the following command to the CLI:

```
head -n 1 /dev/random
```

If a response is returned quickly, */dev/random* can be used as a default random number generator for JVM. If a response is returned over time, perform the following actions to configure JVM to use */dev/urandom*:

1. Open the file *$JAVA_HOME/jre/lib/security/java.security* in a text editor.
2. Replace the following line:

   ```
   securerandom.source=file:/dev/random
   ```

   With this:

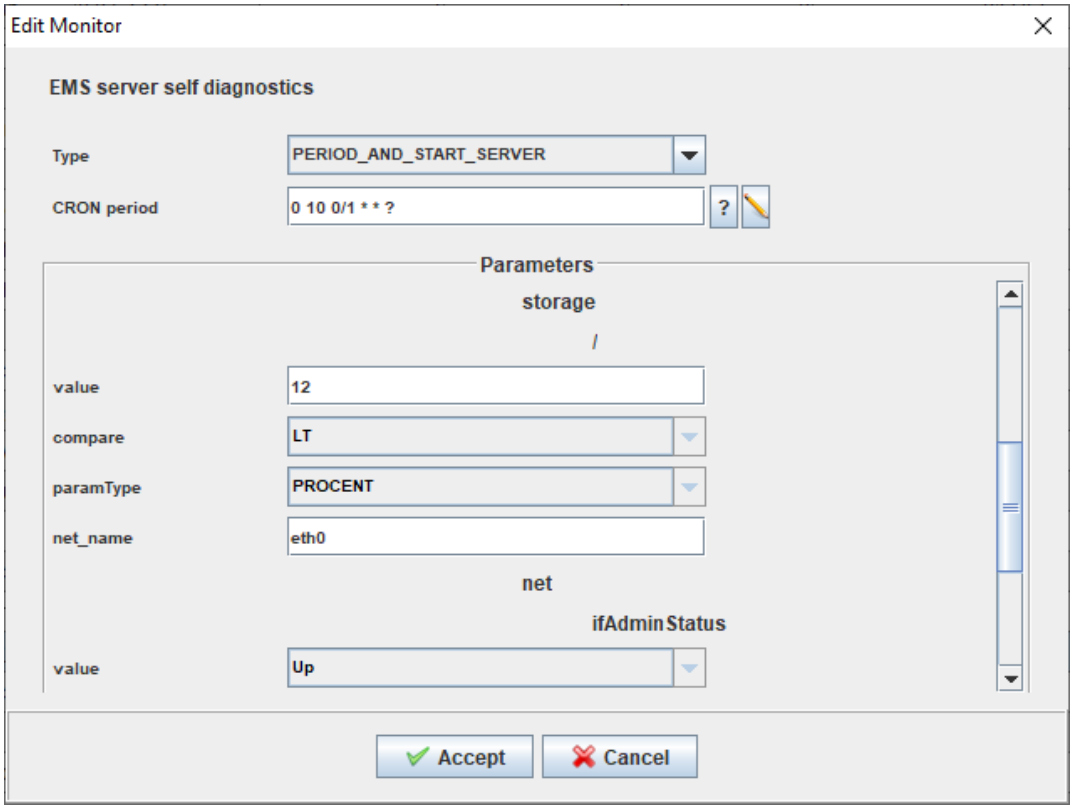
   ```
   securerandom.source=file:/dev/./urandom
   ```

3. Save the changes and exit the editor.

## Solving problems after installation

**"eth0" network interface not found"**

Enter the menu Administration/EMS server configuration/Scheduled tasks (Monitors), select the EMS server self diagnostics monitor (ID=8) and click "Edit".
Edit window of the monitor's parameters will be opened. Replace "net_name" parameter with the name of your interface.




The interface's name can be viewed by running the following command on the server.

```
tester@swlc:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.1  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::523e:aaff:fe05:306f  prefixlen 64  scopeid 0x20<link>
        ether 50:3e:aa:05:30:6f  txqueuelen 1000  (Ethernet)
        RX packets 4711682  bytes 3737032747 (3.7 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2843658  bytes 1607515235 (1.6 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**"DB pool size error: Max DB connections = 151. EMS DB pools max conn info: ont=40; tree=20; wireless=30; syslog=4; event=32; radius=40; Total = 166"The number of connections**

Depending on the estimated number of access points, the maximum number of AP connections should be specified via **max_connections** parameter. It is specified in **/etc/mysql/mysql.conf.d/mysql.cnf** by default, but commented out. Uncomment it and enter the required number, for example, like this:

```
max_connections        = 500
```

Read more in v1.14_MySQL (EN)

## v1.14_SoftWLC multihost system installation

- Installing the ELTEX-PORTAL module
- Installing the ELTEX-WIFI-CAB module
- Installing the ELTEX-PORTAL-CONSTRUCTOR module
- Installing the ELTEX-APB module

## Installing the ELTEX-PORTAL module

Install java
Install eltex-portal
Change the amount of allocated memory and the port number in the configuration file /etc/default/eltex-portal

```
# Eltex-Portal daemon parameters

# Port for use by Eltex Portal
PORT=8080

# Initial size of Java heap
JAVA_INIT_HEAP=256m
# Maximum size of Java heap
JAVA_MAX_HEAP=8096m

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-portal"
```

Change the database URL in the /etc/eltex-portal/config.txt configuration file

```
# Драйвер БД
portal.db.driver=com.mysql.jdbc.Driver
# URL к БД
portal.db.url=jdbc:mysql://<IP_address>:3306/ELTEX_PORTAL?
max_allowed_packet=32362048&useUnicode=true&characterEncoding=utf8
# имя пользователя БД
portal.db.username=javauser
# пароль пользователя БД
portal.db.password=javapassword
```

Restart the eltex-portal service

```
root@vagrant-ubuntu-trusty-64:~# service eltex-portal restart
eltex-portal stop/waiting
eltex-portal start/running, process 14255
root@vagrant-ubuntu-trusty-64:~#
```

Restart tomcat

```
root@vagrant-ubuntu-trusty-64:~# service tomcat7 restart
```

The only thing that should be done now is to configure NGW client and PCRF module access in the Admin Panel. Enter the address http://<ip_address>:8080/wifi-cab/, go to the Settings and select the "Integration" tab.

## Installing the ELTEX-WIFI-CAB module

---

Install java
Install tomcat and set the JAVA_HOME environment variable for tomcat7

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "JAVA_HOME=/usr/lib/jvm/java-8-oracle" >> /etc/
default/tomcat7
```

Add random access memory for java

```
root@vagrant-ubuntu-trusty-64:~# echo "JAVA_OPTS=" -server -Xms2g -Xmx4g -XX:-UseParallelGC -XX:
+UseConcMarkSweepGC -XX:+AggressiveOpts" >> /etc/default/tomcat7
```

Install eltex-oui-list
Install eltex-wifi-cab

Edit the /etc/eltex-wifi-cab/system.xml configuration file, change the addresses to the server with MongoDB installed, to NBI and to SoftWLC eltex-auth-service

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
    <entry key="mongoaddress">mongodb://<IP_address_mongo>:27017/wifi-customer-cab</entry>
    <entry key="nbiaddress">http://<IP_address_NBI>:8080/axis2/services/RadiusNbiService?wsdl</
entry>
    <entry key="nbi.serviceLogin.user">softwlc_service</entry>
    <entry key="nbi.serviceLogin.password">softwlc</entry>
    <entry key="nbi.serviceLogin.requestTimeout.sec">120</entry>
    <!-- параметры, применяемые при авторизации через eltex-auth-service -->
    <entry key="radius.auth.address">IP_address_auth_service</entry>
    <entry key="radius.auth.shareSecret">eltex</entry>
    <entry key="radius.auth.authPort">21812</entry>
    <entry key="radius.auth.acctPort">21813</entry>
    <entry key="radius.auth.timeout.sec">10</entry>
    <entry key="radius.auth.retries">5</entry>
</properties>
```

## Installing the ELTEX-PORTAL-CONSTRUCTOR module

---

The Portal Constructor is usually installed to the same server as the Admin Panel, but if the Portal Constructor is located on a separate server, implement the first 4 paragraphs of the Admin Panel installation guide.
Install the eltex-portal-constructor module and edit the /etc/eltex-portal-constructor/config.txt configuration file where change addresses to eltex-auth-service and mysql database
line 9

```
auth.service.address=<IP_address_auth.service>
```

line 34

```
portal.db.url=jdbc:mysql://<IP_address_mysql>:3306/ELTEX_PORTAL?
max_allowed_packet=32362048&useUnicode=true&characterEncoding=utf8
```

Restart tomcat

```
root@vagrant-ubuntu-trusty-64:~# service tomcat7 restart
```

At this stage, configuration file editing is completed, the only thing left to do is to configure other parameters in the admin panel of the Portal Constructor
Enter the server address http://<ip_address>8080/epadmin/ in a browser's address bar
Open the System settings menu and specify the Portal host and the Portal port in the Portal Constructor tab. Save the changes.Specify the NGW address in the "NGW access" tab. This module is usually installed to the server with EMS. Specify the address of the server with the eltex-radius-nbi module installed (usually the server with EMS) in the "NBI access" tab.Specify the address of the server with eltex-pcrf in the "PCRF access" tab.
Then restart tomcat.

## Installing the ELTEX-APB module

---

Install java
Install eltex-apb
Edit the eltex-radius-nbi configuration file, change the NBI module address

```
nbi.client.protocol=http
nbi.client.host=<IP_address NBI>
nbi.client.port=8080
nbi.client.file=/axis2/services/RadiusNbiService?wsdl
nbi.client.login=softwlc_service
nbi.client.password=softwlc
nbi.client.pool.size=100
```

Then change the amount of RAM allocated for the APB service. Replace the JAVA_MAX_HEAP value with a required one in the etc/default/eltex-apb configuration file
Restart eltex-apb

```
root@vagrant-ubuntu-trusty-64:~# service eltex-apb restart
Stopping eltex-apb ...
eltex-apb stopped
Starting eltex-apb ...
eltex-apb started
root@vagrant-ubuntu-trusty-64:~#
```

# v1.14_SoftWLC backup (EN)


- General information
- Installing and configuring keepalived
- Configuring rsync
  - Starting/stopping procedure
  - Configuring rsync server
  - Configuring synchronization launch
- Configuring MySQL replication
  - Data dump transfer and transfer to the second server
  - MySQL configuration
  - Creating user accounts
  - Starting replication
    - Starting replication on the second server
    - Starting replication on the first server
    - Checking replication from EMS-GUI
- Configuring MongoDB
  - replicaSet configuration
- Eltex-PCRF operation in cluster mode
  - Configuring PCRF cluster
- Configuring SoftWLC modules
- Changing configuration via GUI
  - Admin Panel
  - Portal Constructor
  - EMS-GUI


## General information

SoftWLC controller backup is performed according to the master-slave model. Files critical for system operation (configuration files, firmware files, upload data files), MySQL database files (in master-master mode), MongoDB database files and DHCP server logs are synchronized. Such a model provides service availability and relevance of data on both controllers if one of them fails, network is inaccessible or power supply problems occur.
In configuration examples of this section, IP addresses will be referred to as <ip_server1>, <ip_server2> and <virtual_ip>, where:

- <ip_server1> — real ip address of the first server
- <ip_server2> — real ip address of the second server
- <virtual_ip> — virtual ip address

SoftWLC controllers backup configuration includes the following steps:

- installing and configuring keepalived
- configuring rsync
- Configuring MySQL replication
- configuring replicaSet MongoDB
- configuring Eltex-PCRF operation in cluster mode
- changing configuration of modules for them to use virtual IP

## Installing and configuring keepalived

The main component for controller backup. Provides master role passing and system operation problems detecting. To install keepalived, contact the Wi-Fi Service center and get a relevant distribution kit.

## Configuring rsync

In backup scheme, rsync manages synchronization of Eltex-EMS and Eltex-APB service files, and also firmware, configuration and AP configuration upload files. Rsync is a client-server software. Master server acts as a client and synchronizes slave server's directories with local ones.

### Starting/stopping procedure

To enable rsync server, define the following value in the file **/etc/default/rsync**:

RSYNC_ENABLE=true

To start the service after stopping:

```
root@swlc01-server:/# service rsync start
```

To stop the service, the following command is used:

```
root@swlc01-server:/# service rsync stop
```

To check the service status, use the command:

```
root@swlc01-server:/# service rsync status
```

This will be followed by a message:

```
* rsync is running
```

if the service is running, or by

```
* rsync is not running
```

if it is not.

### Configuring rsync server

The main configuration file of rsync server is located in **`/etc/rsyncd.conf`**. The listing is given below.

**/etc/rsyncd.conf**

```
[ems-conf]
path = /usr/lib/eltex-ems/conf/
use chroot = no
max connections = 2
lock file = /var/lock/rsyncd
read only = no
list = no
uid = root
auth users = backup
secrets file = /etc/rsyncd.secrets
strict modes = yes
# IP-address of the server that will access the resource, i.e., of the second server in the pair
hosts allow = <ip_server1> <virtual_ip>
ignore errors = no
ignore nonreadable = yes
transfer logging = no
timeout = 60
refuse options = checksum dry-run
dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz

[ems-tftp]
path = /tftpboot
use chroot = no
max connections = 2
lock file = /var/lock/rsyncd.tftp
read only = no
list = no
uid = root
auth users = backup
secrets file = /etc/rsyncd.secrets
strict modes = yes
hosts allow = <ip_server1> <virtual_ip>
ignore errors = no
ignore nonreadable = yes
transfer logging = no
timeout = 60
refuse options = checksum dry-run
dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz

[ems-wp]
path = /var/ems-data/WP
use chroot = no
max connections = 2
lock file = /var/lock/rsyncd.ems-wp
read only = no
list = no
uid = root
auth users = backup
```

```
secrets file = /etc/rsyncd.secrets
strict modes = yes
hosts allow = 10.62.8.121 10.62.8.122
ignore errors = no
ignore nonreadable = yes
transfer logging = no
timeout = 60
refuse options = checksum dry-run
dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz
```

**hosts allow** parameters are specified for master server. The following form is recommended:

`hosts allow = <other_server_ip> <virtual ip>`

To perform authentication, configure *rsync* user on both servers by creating files **/etc/rsyncd.secrets** on both servers and specifying login and password in them.

```
backup:rspasswd
```

Assign file access rights by running the following commands on both servers:

```
root@swlc01-server:/# chmod 600 /etc/rsyncd.secrets
```

### Configuring synchronization launch

Create files **/etc/rsync_client.secrets,** specify the following password there:

```
root@swlc01-server:/# echo "rspasswd" > /etc/rsync_client.secrets && chmod 600 /etc/
rsync_client.secrets
```

File synchronization is performed by **cron** task where **/usr/lib/eltex-ems/scripts/rsync_ems_backup.sh** is run**.** The script starts rsync client and synchronizes local directories with directories of the second (backup) server.

Synchronization can be started only if the server works in master state.

**/usr/lib/eltex-ems/scripts/rsync_ems_backup.sh**

```
#!/bin/bash

LOCKFILE="/run/lock/rsync_ems_backup"

# IP address backup server
HOST=<ip_server2>
# Check if we're root
if [ `whoami` != "root" ]
    then
    echo "This script should be run by root."
    exit 1
fi

# Check and create lock file
if ! lockfile-create --use-pid -r 0 $LOCKFILE &> /dev/null ; then
    echo "Backup is already running"
    exit 0
fi

# Check - if we're master - try to perform backup to slave
SRVMODE=`cat /tmp/keep.mode`
if [ "$SRVMODE" == "MASTER" ]
    then
    rsync -urlogtp --delete-after --password-file=/etc/rsync_client.secrets /usr/lib/eltex-ems/
conf/ backup@$HOST::ems-conf > /tmp/rsync_ems_conf.log 2>&1
    echo $? >> /tmp/rsync_ems_conf_result.log
    rsync -urlogtp --delete-after --password-file=/etc/rsync_client.secrets /tftpboot/
 backup@$HOST::ems-tftp > /tmp/rsync_ems_tftpboot.log 2>&1
    echo $? >> /tmp/rsync_ems_tftpboot_result.log
    rsync -urlogtp --delete-after --password-file=/etc/rsync_client.secrets /var/ems-data/WP/
 backup@$HOST::ems-wp > /tmp/rsync_ems_wp.log 2>&1
    echo $? >> /tmp/rsync_ems_wp_result.log
else
    echo "Not master. No action will be performed."
fi

lockfile-remove $LOCKFILE
```

where

- **backup** – login specified in **/etc/rsyncd.secrets** file
- **HOST** – another server's IP address

Create **cron** tasks on both servers to start synchronization every minute:

```
root@swlc01-server:/# crontab -l | { cat; echo "*/1 * * * * /usr/lib/eltex-ems/scripts/
rsync_ems_backup.sh"; } | crontab
```

**cron** service should be started on both servers

## Configuring MySQL replication

Backup of data stored in MySQL database is carried out by master-master replication. That means each server is both master and slave at the same time. The scheme implies writing all database updates of the first server to a special binary log. The second server reads the log and applies the changes. The second server replicates data from the first server, and vice versa (http://dev.mysql.com/doc/refman/5.5/en/replication.html). That allows having a relevant copy of a database on two hosts simultaneously. If connection fails, changes are accumulated and then synchronized after reconnection.

### Data dump transfer and transfer to the second server

When configuring backup during operation (i.e. if the current server's MySQL already has data in it), it is necessary to replicate data to the second server. This can be done using the **mysqldump** utility.
Block the tables, take the dump, unblock the tables and copy the file to the second server:

```
root@swlc01-server:/# mysql -uroot -proot -e "FLUSH TABLES WITH READ LOCK;"
root@swlc01-server:/# mysqldump -uroot -proot --databases ELTEX_PORTAL eltex_alert
eltex_auth_service eltex_ems payments radius wireless > mysqldump_master.sql
root@swlc01-server:/# mysql -uroot -proot -e "UNLOCK TABLES;"
root@swlc01-server:/# scp mysqldump_master.sql <username>@<ip_server2>:/home/<username>/
```

Then generate a dump on the second server:

```
root@swlc01-server:/# mysql -uroot -proot < /home/<username>/mysqldump_master.sql
```

### MySQL configuration

mysql daemon configuration aims at specifying binary logs writing parameters. The words *first server* and *second server* are conditional and used to refer to differences in server configurations.

Make the following changes in **[mysqld]** section of **/etc/mysql/my.cnf** configuration file:

Comment out or delete the following line on both servers:

```
bind-address = 127.0.0.1
```

Specify **server-id**. The servers should be given unique identificators, e.g., for the first server:

```
server-id = 1
```

For the second server:

```
server-id = 2
```

Enable binary logs on both servers:

```
log_bin = /var/log/mysql/mysql-bin.log
```

specify **auto_increment_increment** (increment step) and **auto_increment_offset** (start point) parameters.

For the first server:

```
auto_increment_increment= 2
auto_increment_offset = 1
```

For the second server:

```
auto_increment_increment= 2
auto_increment_offset = 2
```

For both servers:

- specify databases for which logs will be written:

```
binlog-do-db = eltex_alert
binlog-do-db = eltex_ems
binlog-do-db = wireless
binlog-do-db = radius
binlog-do-db = eltex_auth_service
binlog-do-db = ELTEX_PORTAL
binlog-do-db = payments
```

- specify databases for which logs will not be written:

```
binlog-ignore-db = mysql
binlog-ignore-db = Syslog
binlog-ignore-db = performance_schema
binlog-ignore-db = information_schema
```

Restart **mysql** on each server and create a database for replication.

```
root@swlc01-server:/# service mysql restart
```

### Creating user accounts

For replication to work, a service account should be created on both servers. The server will connect master server and get data changes using this account.
Create an account for replication on the first server:

```
GRANT SELECT, REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'replication'@'<ip_server2>'
 IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
```

Create an account for replication on the second server:

```
GRANT SELECT, REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'replication'@'<ip_server1>'
 IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
```

SELECT privilege is used to check replication performance from GUI EMS

### Starting replication

#### Starting replication on the second server

Run the **show master status** command in MySQL console of the **first** server and analyze the values obtained:

```
mysql> show master status \G

*************************** 1. row ***************************
            File: mysql-bin.000001
        Position: 00000107
    Binlog_Do_DB: eltex_alert,eltex_ems,radius,wireless,eltex_auth_service,payments,ELTEX_PORTAL
Binlog_Ignore_DB: mysql,Syslog,performance_schema,information_schema
1 row in set (0.00 sec)
```

Remember the parameters **File** and **Position.**

> It is recommended to set **Position** equal to 107. This is the position from which log file writing begins.

Configure and start the **second** server replication from the first one **(perform the following operations on the second server):**

```
mysql>  STOP SLAVE;
mysql>  CHANGE MASTER TO MASTER_HOST='<ip_server1>', MASTER_USER='replication',
MASTER_PASSWORD='password', MASTER_LOG_FILE='mysql-bin.000001', MASTER_LOG_POS=107;
mysql>  START SLAVE;
```

where

- MASTER_LOG_FILE=**'mysql-bin.000001'** – specify **File** value, got on the first server.
- MASTER_LOG_POS=**107** – specify **Position** value, got on the previous step (on the initial setting, 107 is recommended).

Check replication state on the second server:

```
mysql> show slave status \G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: <ip_server1>
                  Master_User: replication
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000001
          Read_Master_Log_Pos: 107
               Relay_Log_File: mysqld-relay-bin.000001
                Relay_Log_Pos: 107
        Relay_Master_Log_File: mysql-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Master_Log_Pos: 107
              Relay_Log_Space: 107
              Until_Condition: None
               Until_Log_File:
                Until_Log_Pos: 0
           Master_SSL_Allowed: No
           Master_SSL_CA_File:
           Master_SSL_CA_Path:
              Master_SSL_Cert:
            Master_SSL_Cipher:
               Master_SSL_Key:
        Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 2
1 row in set (0.00 sec)
```

If **`Slave_IO_Running`** and **`Slave_SQL_Running`** are set to **«Yes»,** replication has been started successfully.

Starting replication on the first server

On the second server run:

```
show master status \G
mysql> show master status \G

*************************** 1. row ***************************
            File: mysql-bin.000001
        Position: 00000107
    Binlog_Do_DB:
eltex_alert,eltex_ems,eltex_ont,radius,wireless,eltex_auth_service,payments,ELTEX_PORTAL
Binlog_Ignore_DB: mysql,Syslog,performance_schema,information_schema
1 row in set (0.00 sec)
```

Configure and start first server replication from the second server **(run the following commands on the first server):**

```
CHANGE MASTER TO MASTER_HOST='<ip_server2>', MASTER_USER='replication',
MASTER_PASSWORD='password', MASTER_LOG_FILE='mysql-bin.000001', MASTER_LOG_POS=107;
START SLAVE;
```

Check replication state on the first server:

```
mysql> show slave status \G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: <ip_server2>
                  Master_User: replication
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000001
          Read_Master_Log_Pos: 107
               Relay_Log_File: mysqld-relay-bin.000001
                Relay_Log_Pos: 107
        Relay_Master_Log_File: mysql-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
...
```

*the output given is incomplete, since other data is less important*
If **`Slave_IO_Running`** and **`Slave_SQL_Running`** parameters are set to **«Yes»**, **`Master_Log_File`** and **`Read_Master_Log_Pos`** values are given, replication is performed in both directions.

Checking replication from EMS-GUI

MySQL replication state can be controlled from GUI EMS. To do that, edit **`/etc/eltex-ems/check-ems-replication.conf`** configuration file. The changes should be made on both servers:

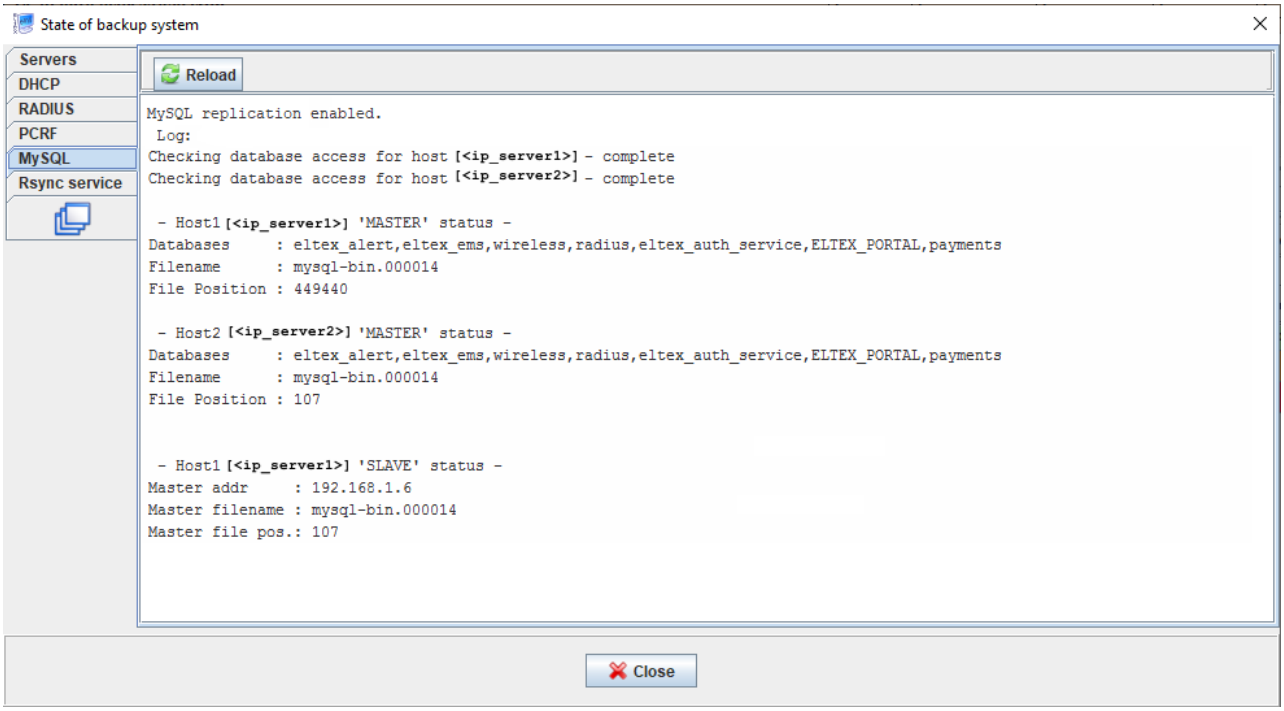
**/etc/eltex-ems/check-ems-replication.conf**

```
# Enable("Yes") / Disable("No") replication check
ENABLE_REPLICATION="Yes"

# The first replication host's address
HOST1=<ip_server1>
# The second replication host's address
HOST2=<ip_server2>


# mysql server access parameters
# mysql user
USER="replication"
# mysql password
PASSWORD="password"
```

where

- **ENABLE_REPLICATION** shows whether replication check is enabled (set to "Yes")
- **`HOST1, HOST2`** - servers' IP addresses
- **`USER, PASSWORD`** - user account login/password for replication.

After saving the changes, replication state can be checked via GUI EMS in *Information → State of backup system → MySQL*.




Results of replication state check on both servers and brief summary of check results are given in the section.

## Configuring MongoDB

In MongoDB, replication is performed via grouping several (3 for standart configuration) nodes into Replica Set. Replica Set consists of one Primary node and several Secondary nodes (more information on https://docs.mongodb.com/v2.4/administration/replica-sets.

**All** data change operations are performed **only** on Primary. Thus, MongoDB automatically performs failover and replaces Primary with a working node if current Primary fails. But that requires 3+ nodes in Replica Set.

**In the default configuration, Replica Set that consists of two nodes completely goes down when a failure in one of them (even in Secondary)**.

### replicaSet configuration

In **`/etc/mongodb.conf`** on both nodes:
add the line

```
replSet = <replica_set_name>
```

where **<replica_set_name>** is a name of replica set, which is chosen arbitrarily but should be the same for both servers.
Comment out or delete the line:

```
# bind_ip = 127.0.0.1
```

Restart MongoDB

```
root@swlc01-server:/# service mongodb restart
```

Open MongoDB console on the first node

```
root@swlc01-server:/#  mongo
```

Create replica set configuration

```
> rs.initiate()
```

After a while, shell prompt should be changed to:

```
replica_set_name:PRIMARY>
```

If DNS is not used in the network, check if the first node was successfully added to Replica Set configuration.

```
replica_set_name:PRIMARY> rs.config()
{
    "_id" : "replica_set_name",
    "version" : 63243,
    "members" : [
        {
            "_id" : 0,
            "host" : "<hostname_server1>:27017"
        }
    ]
}
```

If the first element (at index 0) has hostname instead of IP address, and DNS is not used in the network, Replica Set configuration should be updated before adding the second node. If DNS is used, and DNS name is correct, the second node can be added.

To update the server's address, run the following commands:

```
replica_set_name:PRIMARY> conf = rs.conf()
replica_set_name:PRIMARY> conf.members[<индекс>].host = "<ip_server1>:27017"
replica_set_name:PRIMARY> rs.reconfig(conf)
```

Check the current configuration again:

```
replica_set_name:PRIMARY> rs.config()
{

    "_id" : "relica_set_name",
    "version" : 63243,
    "members" : [
        {
            "_id" : 0,
            "host" : "<ip_server1>:27017"
        }
    ]
}
```

**"host"** parameter should contain the server's IP address.

Add the second node to Replica Set (run on the first server):

```
replica_set_name:PRIMARY> rs.add("<ip_server2>")
{ "ok" : 1 }
```

MongoDB error response can be generated if there is no connection to the second node (or bind_ip = 127.0.0.1 is specified there), or replSet is not configured .On the second node, MongoDB management console prompt should be changed to:

```
root@swlc01-server:/# mongo
replica_set_name:SECONDARY>
```

The same should be done for other nodes. Replica Set state can be checked by running the command **rs.status()** in MongoDB console.

## Eltex-PCRF operation in cluster mode

### Configuring PCRF cluster

Open 5701 tcp and 5801 tcp ports between PCRF servers
On servers, in **/etc/eltex-pcrf/hazelcast-cluster-network.xml** configuration files, specify

network interfaces' addresses (lines 5 and 22 of the example contain the server's address, and lines 14 and 15 contain the list of all cluster members).

Configuration example:

```
1   <network>
2       <!-- Write here public address of the node -->
3
4       <!-- specify the server's own address here -->
5       <public-address>ip_server1</public-address>
6       <port auto-increment="false" port-count="100">5701</port>
7       <outbound-ports>
8           <ports>0</ports>
9       </outbound-ports>
10      <join>
11          <multicast enabled="false"/>
12          <tcp-ip enabled="true">
13              <!-- List IP addresses of all cluster members (including this one) -->
14              <member>ip_server1</member>
15              <member>ip_server2</member>
16          </tcp-ip>
17          <discovery-strategies>
18          </discovery-strategies>
19      </join>
20      <interfaces enabled="true">
21      <!-- specify the server's own address here -->
22          <interface>ip_server1</interface>
23      </interfaces>
```

Permit cluster start in **/etc/eltex-pcrf/eltex-pcrf.json** configuration file:

```
"cluster.enable" : true,
```

Restart Eltex-PCRF using the command

```
root@swlc01-server:/# service eltex-pcrf restart
```

Cluster state check

- http://<ip_server1>:7070/cluster
- http://<ip_server2>:7070/cluster

```
{
  "data" : {
    "enabled" : true,
    "state" : "ACTIVE",
    "members" : [ {
      "address" : "ip_server1",
      "local" : true,
      "active" : true
    }, {
      "address" : "ip_server2",
      "local" : false,
      "active" : true
    } ],
    "messagesStats" : {
      "received" : 45157,
      "sent" : 45144
    },
    "mongo" : {
      "available" : false,
      "error" : "not running with --replSet"
    }
  },
  "key" : "PcrfErrorCode.success",
  "message" : "Success",
  "code" : 0,
  "args" : [ ]
}
```


## Configuring SoftWLC modules

It is necessary to configure SoftWLC modules on both servers to interact with controller via virtual ip. The following configuration files should be changed:

**Файл /etc/eltex-apb/apb.properties**

```
1  nbi.client.protocol=http
2  nbi.client.host=localhost
3  nbi.client.port=8080
4  nbi.client.file=/axis2/services/RadiusNbiService?wsdl
5  nbi.client.login=admin
6  nbi.client.password=password
7  nbi.client.pool.size=100
8
9  # Config filePath to cache
10 cache.config=/etc/eltex-apb/ehcache.xml
11
12 # list of permitted files to
13 hosts.file=/etc/eltex-apb/hosts.json
14
15 # RRM config
16 rrm.conf.file=/etc/eltex-apb/rrmconf.json
17
18 # Timeout waiting for subscribe-request after connecting the access point to the server,
   in seconds
19 subscribe.idle.timeout=60
```

- Change **localhost** to **<virtual_ip>** in line 2.

**Файл /etc/eltex-pcrf/eltex-pcrf.json**

```
{
  "auth.address" : "0.0.0.0",
  "auth.port" : 31812,
  "auth.mac.open.timeout.s" : 3600,
  "auth.mac.welcome.service" : "WELCOME",

  "acct.address" : "0.0.0.0",
  "acct.port" : 31813,

  "lease.saver.address" : "0.0.0.0",
  "lease.saver.port" : 4381,

  "aaa.instances" : 5,
  "aaa.host" : "127.0.0.1",
  "aaa.secret" : "testing123",
  "aaa.auth.port" : 1812,
  "aaa.acct.port" : 1813,
  "aaa.rest.port" : 7080,
  "aaa.timeout" : 10,
  "aaa.attempts" : 1,

  "web.monitoring.port" : 7070,

  "cluster.enable" : false,
  "cluster.eventBusPort" : 5801,

  "radius" : {
    "url" : "jdbc:mysql://localhost/radius?
useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReco
nnect=true",
    "user" : "javauser",
    "password" : "javapassword",
    "max_pool_size" : 16
  },

  "mongo.pcrf" : {
    "connection_string": "mongodb://localhost:27017/pcrf",
    "db_name": "pcrf"
  },

  "session.storage" : {
    "session.check.period.s" : 300,
    "unauth.store.time.s" : 600,
    "interval.number.expired" : 3,
    "min.interval.s" : 45,
    "default.interval.s" : 600
  },

```

```
47
48  "bras.coa" : {
49      "coa.timeout" : 10,
50      "coa.attempts" : 1,
51      "remote.coa.port" : 3799,
52      "executor.size" : 100,
53      "log.clean.period.s" : 600,
54      "log.store.period" : {
55        "period" : 14,
56        "unit" : "D"
57      }
58    },
59
60    "sql.ems" : {
61      "url" : "jdbc:mysql://localhost/eltex_ems?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReco
    nnect=true",
62      "user" : "javauser",
63      "password" : "javapassword",
64      "max_pool_size" : 16
65    },
66
67    "sql.wireless" : {
68      "url" : "jdbc:mysql://localhost/wireless?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReco
    nnect=true",
69      "user" : "javauser",
70      "password" : "javapassword",
71      "max_pool_size" : 16
72    }
73
74  }
```

- Change **`localhost`** to **`<virtualip>`** in lines 28, 35, 61, 68.

**Файл /etc/eltex-portal-constructor/config.txt**

```
# The number of attempts to log into Admin Panel before locking.
admin.attempts=5
# The number of minutes after reaching the maximum number of attempts to log into Admin Panel
admin.block.time=5

################################################################################
#######################Eltex Auth Service settings##############################
################################################################################
auth.service.address=localhost
auth.service.port=21812
auth.service.timeout=10
auth.service.secret=eltex
auth.service.retries=3
# pap, chap, mschapv2, eap-mschapv2, eap-md5, eap-ttls
auth.service.protocol=eap-md5

################################################################################
#############################DB ELTEX_PORTAL settings###########################
################################################################################
# SQL dialect corresponding to DB type
portal.hibernate.dialect=org.hibernate.dialect.MySQL5Dialect
# Use level 2 cache
portal.hibernate.use_second_level_cache=true
# use sql request caching
portal.hibernate.use_query_cache=true
# selecting neighbouring entities
portal.hibernate.batch_size=2
# the number of entries after the first iteration
portal.hibernate.fetch_size=100
# Show the generated sql
portal.hibernate.show_sql=false
################################################################################
# DB driver
portal.db.driver=com.mysql.jdbc.Driver
# DB URL
portal.db.url=jdbc:mysql://localhost:3306/ELTEX_PORTAL?max_allowed_packet=32362048&useUnicode=true&characterEncoding=utf8
# DB user's name
portal.db.username=javauser
# DB user's password
portal.db.password=javapassword
# request by pool to check connection validity
portal.db.validationQuery=select 1
# connection check period
portal.db.validationQueryTimeout=500
# a checkbox showing if a connection should be checked when being received from a pool
portal.db.testOnBorrow=true
```

```
47  # a checkbox showing if a connection should be checked when being returned to a pool
48  portal.db.testOnReturn=false
49  # a checkbox showing if a connection should be checked while idle
50  portal.db.testWhileIdle=true
51  # the number of ms at the borrow moment
52  portal.db.maxWait=10000
53  # minimum number of connections
54  portal.db.initialSize=1
55  # maximum number of connections
56  portal.db.maxActive=20
57  # maximum number of idle connections
58  portal.db.maxIdle=1
59  # minimum number of idle connections
60  portal.db.minIdle=1
61  # time between validity check cycles
62  portal.db.timeBetweenEvictionRunsMillis=10000
63  # minimum idle time
64  portal.db.minEvictableIdleTimeMillis=2000
65  # setting AutoCommit for connection
66  portal.db.defaultAutoCommit=false
```

Change **localhost** to **<virtualip>** in the lines 9, 36.

**Файл /etc/eltex-portal/config.txt**

```
# DB ELTEX_PORTAL
# SQL dialect corresponding to DB type
portal.hibernate.dialect=org.hibernate.dialect.MySQL5Dialect
# Use level 2 cache
portal.hibernate.use_second_level_cache=true
# use sql request caching
portal.hibernate.use_query_cache=true
# selecting neighbouring entities
portal.hibernate.batch_size=1
# the number of entries after the first iteration
portal.hibernate.fetch_size=100
# Show the generated sql
portal.hibernate.show_sql=false

# DB driver
portal.db.driver=com.mysql.jdbc.Driver
# DB URL
portal.db.url=jdbc:mysql://localhost:3306/ELTEX_PORTAL?
max_allowed_packet=32362048&useUnicode=true&characterEncoding=utf8
# database user's name
portal.db.username=javauser
# database user's password
portal.db.password=javapassword
# request by pool to check connection validity
portal.db.validationQuery=select 1
# connection check period
portal.db.validationQueryTimeout=500
# a checkbox showing if a connection should be checked when being received from a pool
portal.db.testOnBorrow=true
# a checkbox showing if a connection should be checked when being returned to a pool
portal.db.testOnReturn=false
# a checkbox showing if a connection should be checked while idle
portal.db.testWhileIdle=true
# the number of ms at the borrow moment
portal.db.maxWait=10000
# minimum number of connections
portal.db.initialSize=5
# maximum number of connections
portal.db.maxActive=50
# maximum number of idle connections
portal.db.maxIdle=5
# minimum number of idle connections
portal.db.minIdle=1
# time between validity check cycles
portal.db.timeBetweenEvictionRunsMillis=10000
# minimum idle time
portal.db.minEvictableIdleTimeMillis=2000
# setting AutoCommit for connection
```

```
48 portal.db.defaultAutoCommit=false
49
50 portal.global_redirect_url=http://eltex-co.ru/
```

Change **localhost** to **<virtualip>** in line 18.

**Файл /etc/eltex-radius-nbi/radius_nbi_config.txt**

```
# DB  radius(alias=radius)
radius.jdbc.driver=org.gjt.mm.mysql.Driver
radius.jdbc.dbUrl=jdbc:mysql://localhost/radius?zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
radius.jdbc.username=javauser
radius.jdbc.password=javapassword
radius.jdbc.maxPoolSize=48
radius.jdbc.inUse=yes

# DB ems(alias=ems)
ems.jdbc.driver=org.gjt.mm.mysql.Driver
ems.jdbc.dbUrl=jdbc:mysql://localhost/eltex_ems?zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&noAccessToProcedureBodies=true
ems.jdbc.username=javauser
ems.jdbc.password=javapassword
ems.jdbc.maxPoolSize=48
ems.jdbc.inUse=yes

# DB  wireless (alias=wireless)
wireless.jdbc.driver=org.gjt.mm.mysql.Driver
wireless.jdbc.dbUrl=jdbc:mysql://localhost/wireless?zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
wireless.jdbc.username=javauser
wireless.jdbc.password=javapassword
wireless.jdbc.maxPoolSize=48
wireless.jdbc.inUse=yes

# DB logs (alias=logs)
logs.jdbc.driver=org.gjt.mm.mysql.Driver
logs.jdbc.dbUrl=jdbc:mysql://localhost/eltex_alert?zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
logs.jdbc.username=javauser
logs.jdbc.password=javapassword
logs.jdbc.maxPoolSize=48
logs.jdbc.inUse=yes

# DB logs (alias=eltex_auth_service)
eltex_auth_service.jdbc.driver=org.gjt.mm.mysql.Driver
eltex_auth_service.jdbc.dbUrl=jdbc:mysql://localhost/eltex_auth_service?zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
eltex_auth_service.jdbc.username=javauser
eltex_auth_service.jdbc.password=javapassword
eltex_auth_service.jdbc.maxPoolSize=48
```

```
eltex_auth_service.jdbc.inUse=no

# адрес ems-northbound
ems.nbi.host=127.0.0.1
ems.nbi.port=8080
ems.nbi.path=northbound
ems.nbi.protocol=http

# eltex_auth_service
auth.port=22
auth.host=127.0.0.1
auth.username=username
auth.password=password

# freeradius-domain-1
freeradius-domain-1.port=22
freeradius-domain-1.host=192.168.0.1
freeradius-domain-1.username=username
freeradius-domain-1.password=password

# freeradius-domain-2
freeradius-domain-2.port=22
freeradius-domain-2.host=192.168.0.2
freeradius-domain-2.username=username
freeradius-domain-2.password=password

# tomcat url
tomcat.host=172.27.1.18
tomcat.port=8080

# pcrf stuff
pcrf.enabled=true
pcrf.url=http://localhost:7070
pcrf.username=admin
pcrf.password=password

# pcrf mongodb connector
pcrf.mongodb.enabled=true
pcrf.mongodb.uri=mongodb://localhost:27017/pcrf

# wifi-customer-cab mongodb connector
wificab.mongodb.enabled=true
wificab.mongodb.uri=mongodb://localhost:27017/wifi-customer-cab

# Eltex.SORM2.replicator MongoDB 'sorm2' connect
sorm2.mongodb.enabled=false
sorm2.mongodb.uri=mongodb://localhost:27017/sorm2

# Eltex.SORM2.replicator host to use API
sorm2.enabled=false
sorm2.url=http://localhost:7071
```

```
90  sorm2.username=admin
91  sorm2.password=password
92
93  #It enables records export to SORM3 while editing wifi users
94  sorm3.enabled=false
95
96  ################################################################################
97  ##########################DB ELTEX_PORTAL settings##############################
98  ################################################################################
99  portal.db.driver=com.mysql.jdbc.Driver
100 portal.db.dialect=org.hibernate.dialect.MySQL5Dialect
101 portal.db.url=jdbc:mysql://localhost:3306/ELTEX_PORTAL?
    max_allowed_packet=32362048&useUnicode=true&characterEncoding=utf8
102 portal.db.username=javauser
103 portal.db.password=javapassword
104 portal.hibernate.use_second_level_cache=false
105 portal.hibernate.use_query_cache=false
```

- Change **`localhost`** to **`<virtualip>`** in lines 3, 11, 19, 27, 35, 71, 77, 81, 85, 101
- Change **`127.0.0.1`** to **`<virtualip>`** in lines 49, 66

**Файл /etc/eltex-ngw/notification.properties**

```
1  #Common gates settings
2  #Current gate used for each type (config name, for example smpp_gate.conf)
3  sms.gate.outgoing.sms.config=smsc_gate.conf
4  #For incoming sms/calls fields for numbers in configs should be set
5  sms.gate.incoming.sms.config=
6  sms.gate.incoming.call.config=
7
8  #Gate pool settings
9  sms.gate.pool.size=50
10 sms.gate.pool.wait.millis=5000
11
12 #Port to listen for requests
13 server.port=8040
14
15 #==============================
16 #=======database settings=====
17 #==============================
18 #mongodb.uri=mongodb://192.168.1.1,192.168.1.2:27017/notification-gw
19 mongodb.host=localhost
20 mongodb.port=27017
21 #mongodb.user=user
22 #mongodb.password=password
23 mongodb.name=notification-gw
24
25 #==============================
26 #=======email settings========
27 #==============================
28 mail.smtp.submitter=test@email.com
29 mail.smtp.password=
30 mail.smtp.auth=true
31 mail.smtp.host=email.com
32 mail.smtp.port=587
33 mail.smtp.sendpartial=true
34 mail.smtp.starttls.enable=false
35 mail.smtp.connectiontimeout=5000
36 mail.gate.pool.size=20
37 mail.pool.wait.millis=10000
```

- Change **`localhost`** to **`<virtualip>`** in line 19

**Файл /etc/eltex-radius/local.conf**

```
# Ports on which the server will listen
auth_port=1812
acct_port=1813
inner_tunnel_port=18121

# MySQL database
db_host="localhost"
db_port=3306
db_login="radius"
db_password="radpass"
db_name="radius"

# Enable checking that SSID is locked (1 - enabled, other values - disabled)
# Check is performed using query to 'wireless' database
ssid_check_enabled=1

# MySQL 'wireless' database
wireless_db_host="localhost"
wireless_db_port=3306
wireless_db_login="javauser"
wireless_db_password="javapassword"
wireless_db_name="wireless"

# PCRF
pcrf_host="127.0.0.1"
pcrf_port=7080
pcrf_enabled=1

# EAP
ca_cert_name="default.pem"
tls_key_password="eltex"

# Proxying
proxy_auth=0
proxy_domain_regex="^(.+\.)?enterprise\.root$"
proxy_host="127.0.0.1"
proxy_port=18121
proxy_secret="eltex"

# Ubiquity vendor detection
ubi_vendor_regex="Apple|Ubiquiti"

# Settings of runtime NAS discovery
dynamic_clients=false
dynamic_client_subnet=192.168.0.0/16
dynamic_client_lifetime=3600
dynamic_client_rate_limit=false
```

- Change **`localhost`** to **`<virtualip>`** in lines 7, 18
- Change **`127.0.0.1`** to **`<virtualip>`** in line 25

**Файл /etc/eltex-wifi-cab/system.xml**

```
1  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
2  <!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
3  <properties>
4      <entry key="mongoaddress">mongodb://localhost:27017/wifi-customer-cab</entry>
5      <entry key="nbiaddress">http://172.27.1.18:8080/axis2/services/RadiusNbiService?
   wsdl</entry>
6      <entry key="nbi.serviceLogin.user">softwlc_service</entry>
7      <entry key="nbi.serviceLogin.password">softwlc</entry>
8      <!-- параметры, применяемые при авторизации через eltex-auth-service -->
9      <entry key="radius.auth.address">localhost</entry>
10     <entry key="radius.auth.shareSecret">eltex</entry>
11     <entry key="radius.auth.authPort">21812</entry>
12     <entry key="radius.auth.acctPort">21813</entry>
13     <entry key="radius.auth.timeout.sec">10</entry>
14     <entry key="radius.auth.retries">5</entry>
15 </properties>
```

- Change **`localhost`** to **`<virtualip>`** in lines 4, 5, 9

**Файл /usr/lib/eltex-ems/conf/config.txt**

```
# DB Event
poolName1=event
event.jdbc.driver=org.gjt.mm.mysql.Driver
event.jdbc.dbUrl=jdbc:mysql://localhost/eltex_alert?useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
event.jdbc.username=javauser
event.jdbc.password=javapassword
event.jdbc.maxPoolSize=32
event.jdbc.inUse=yes
# remote db host access with su privileges
# event.ssh.login=
# event.ssh.password=
# event.ssh.port=

# DB Tree
poolName2=tree
tree.jdbc.driver=org.gjt.mm.mysql.Driver
tree.jdbc.dbUrl=jdbc:mysql://localhost/eltex_ems?useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&noAccessToProcedureBodies=true
tree.jdbc.username=javauser
tree.jdbc.password=javapassword
tree.jdbc.maxPoolSize=20
tree.jdbc.inUse=yes

# DB Ont
poolName3=ont
ont.jdbc.driver=org.gjt.mm.mysql.Driver
ont.jdbc.dbUrl=jdbc:mysql://localhost/eltex_ont?useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
ont.jdbc.username=javauser
ont.jdbc.password=javapassword
ont.jdbc.maxPoolSize=40
ont.jdbc.inUse=yes

# DB Syslog
poolName4=syslog
syslog.jdbc.driver=org.gjt.mm.mysql.Driver
syslog.jdbc.dbUrl=jdbc:mysql://localhost/Syslog?useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
syslog.jdbc.username=javauser
syslog.jdbc.password=javapassword
syslog.jdbc.maxPoolSize=4
syslog.jdbc.inUse=yes
# remote db host access with su privileges
# syslog.ssh.login=
# syslog.ssh.password=
# syslog.ssh.port=
```

```
44
45  # DB acsmain (alias=cpe)
46  poolName5=cpe
47  cpe.jdbc.driver=org.gjt.mm.mysql.Driver
48  cpe.jdbc.dbUrl=jdbc:mysql://localhost/acsmain?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
49  cpe.jdbc.username=javauser
50  cpe.jdbc.password=javapassword
51  cpe.jdbc.maxPoolSize=2
52  cpe.jdbc.inUse=yes
53
54  # DB  acscmds(alias=cmds)
55  poolName6=cmds
56  cmds.jdbc.driver=org.gjt.mm.mysql.Driver
57  cmds.jdbc.dbUrl=jdbc:mysql://localhost/acscmds?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
58  cmds.jdbc.username=javauser
59  cmds.jdbc.password=javapassword
60  cmds.jdbc.maxPoolSize=2
61  cmds.jdbc.inUse=yes
62
63  # DB  acsinf(alias=inf)
64  poolName7=inf
65  inf.jdbc.driver=org.gjt.mm.mysql.Driver
66  inf.jdbc.dbUrl=jdbc:mysql://localhost/acsinf?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
67  inf.jdbc.username=javauser
68  inf.jdbc.password=javapassword
69  inf.jdbc.maxPoolSize=2
70  inf.jdbc.inUse=yes
71
72  # DB  acscache(alias=cache)
73  poolName8=cache
74  cache.jdbc.driver=org.gjt.mm.mysql.Driver
75  cache.jdbc.dbUrl=jdbc:mysql://localhost/acscache?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
76  cache.jdbc.username=javauser
77  cache.jdbc.password=javapassword
78  cache.jdbc.maxPoolSize=2
79  cache.jdbc.inUse=yes
80
81  # DB  radius(alias=radius)
82  poolName9=radius
83  radius.jdbc.driver=org.gjt.mm.mysql.Driver
84  radius.jdbc.dbUrl=jdbc:mysql://localhost/radius?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
85  radius.jdbc.username=javauser
86  radius.jdbc.password=javapassword
87  radius.jdbc.maxPoolSize=40
88  radius.jdbc.inUse=yes
89  # remote db host access with su privileges
```

```
90  # radius.ssh.login=
91  # radius.ssh.password=
92  # radius.ssh.port=
93
94  # ------------------------------------------ SSID
    ------------------------------------------
95  # DB  wireless (alias=wireless)
96  poolName10=wireless
97  wireless.jdbc.driver=org.gjt.mm.mysql.Driver
98  wireless.jdbc.dbUrl=jdbc:mysql://localhost/wireless?
    useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000
99  wireless.jdbc.username=javauser
100 wireless.jdbc.password=javapassword
101 wireless.jdbc.maxPoolSize=30
102 wireless.jdbc.inUse=yes
```

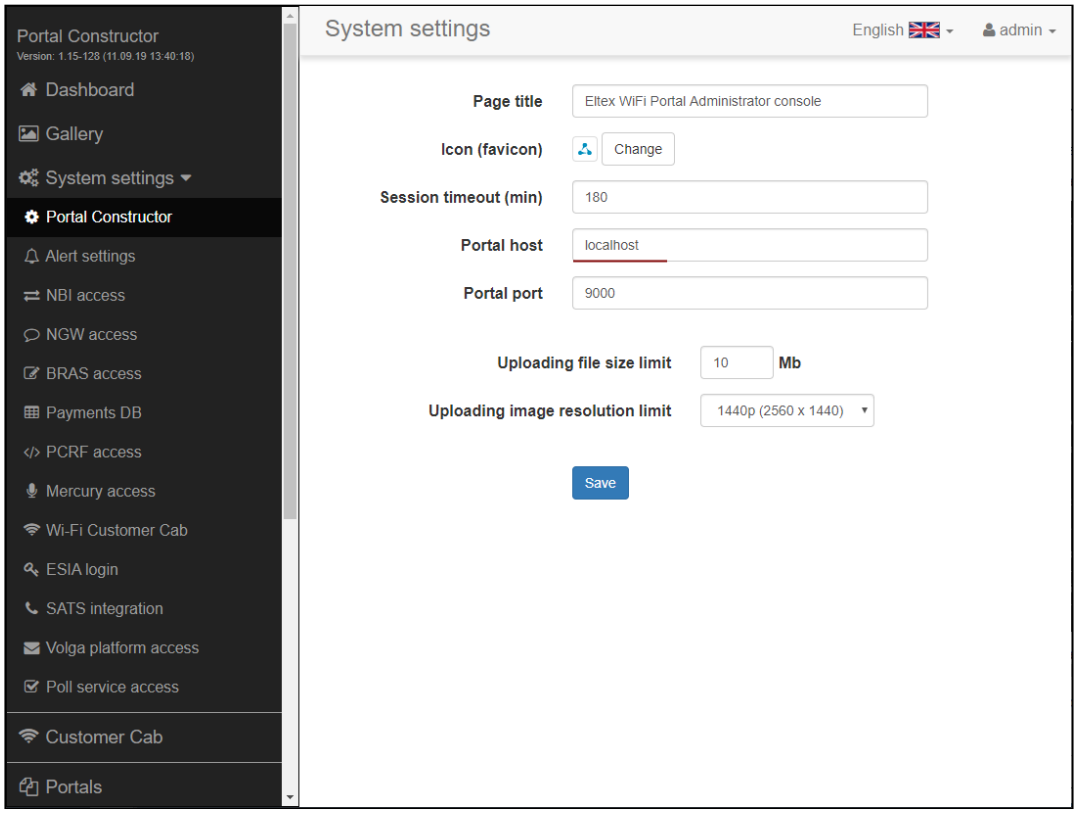
Change **localhost** to **<virtualip>** in the lines 4, 17, 26, 35, 48, 57, 66, 75, 84, 98

## Changing configuration via GUI

SoftWLC modules should also be configured via graphical interface.

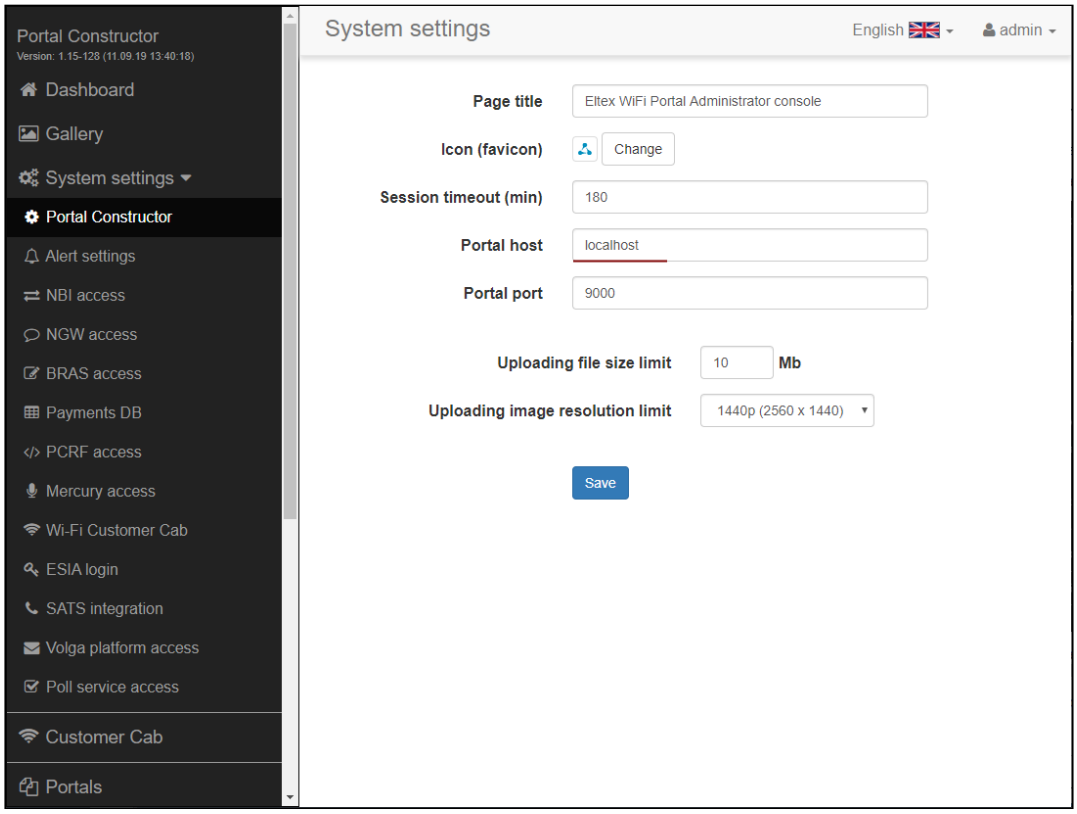
### Admin Panel

In the section *Settings → Integration* replace localhost with a virtual IP address in *PCRF URL* and *URL NGW-клиента* parameters:

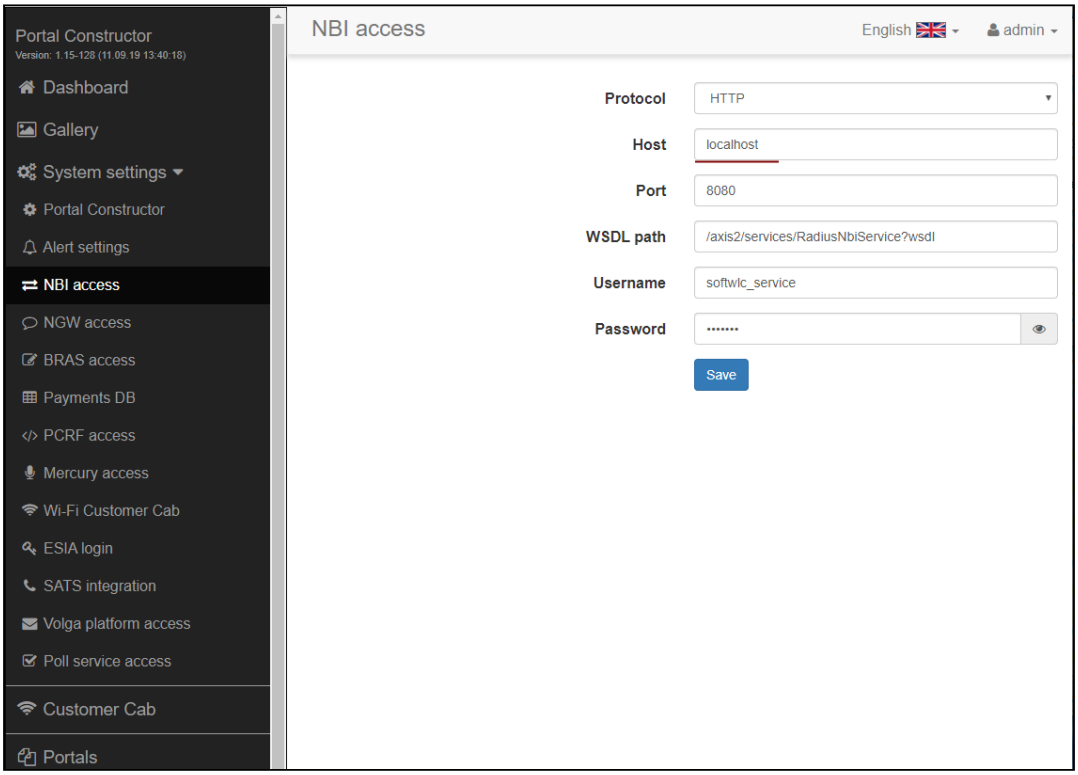



## Portal Constructor

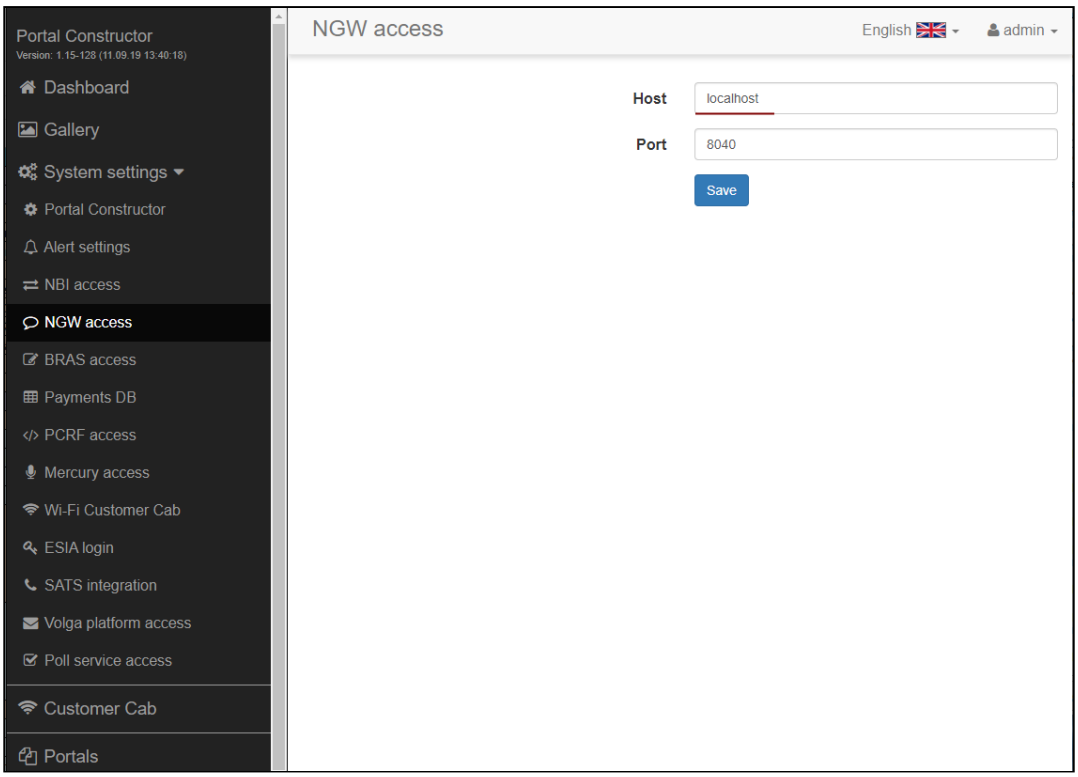
Replace localhost with a virtual IP address in the following sections:
System settings → Portal Constructor



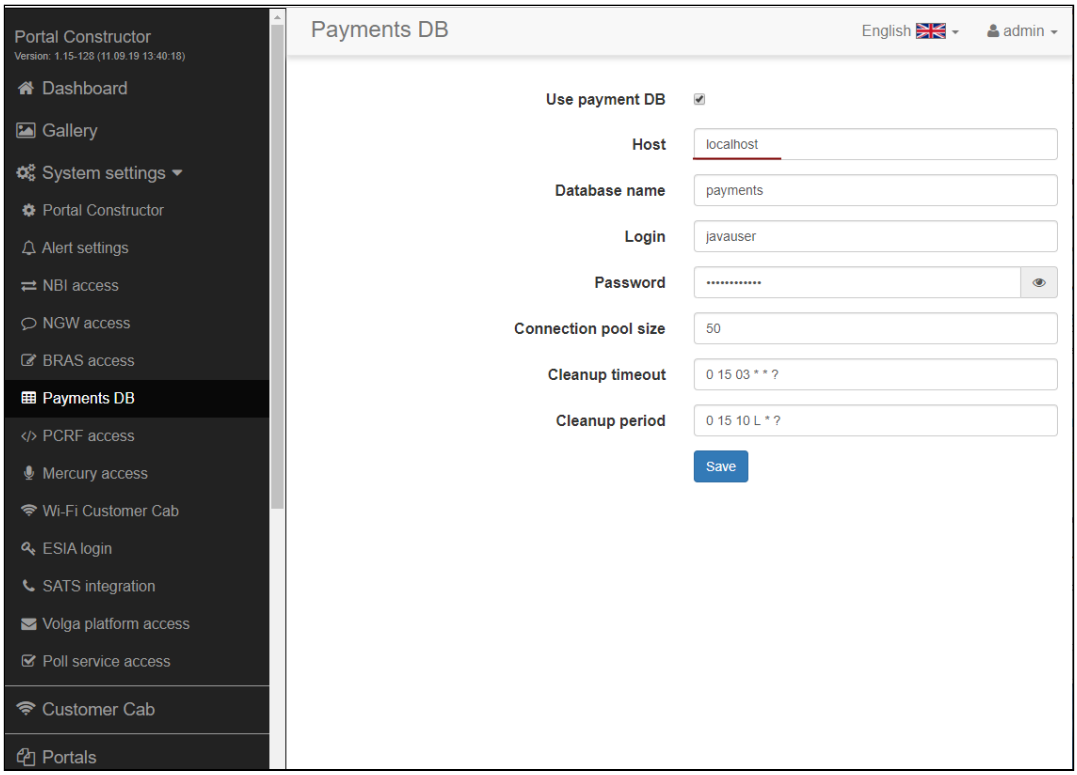

System settings → NBI access



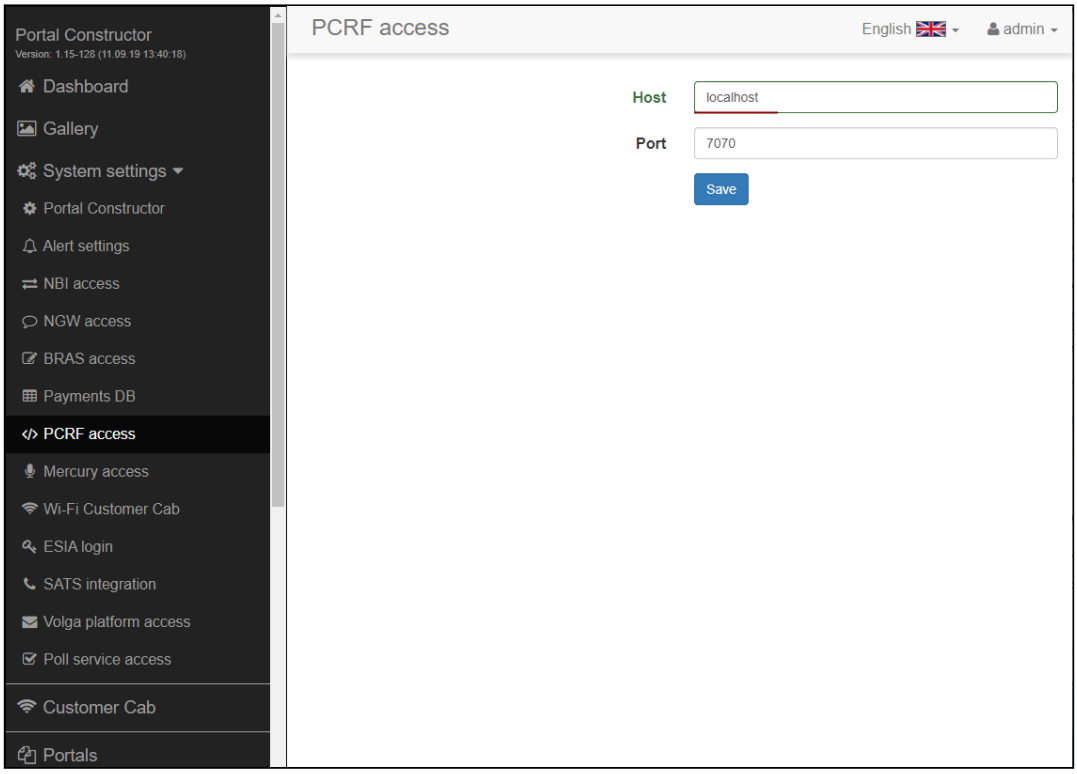
System settings → NGW access




System settings → Payments DB

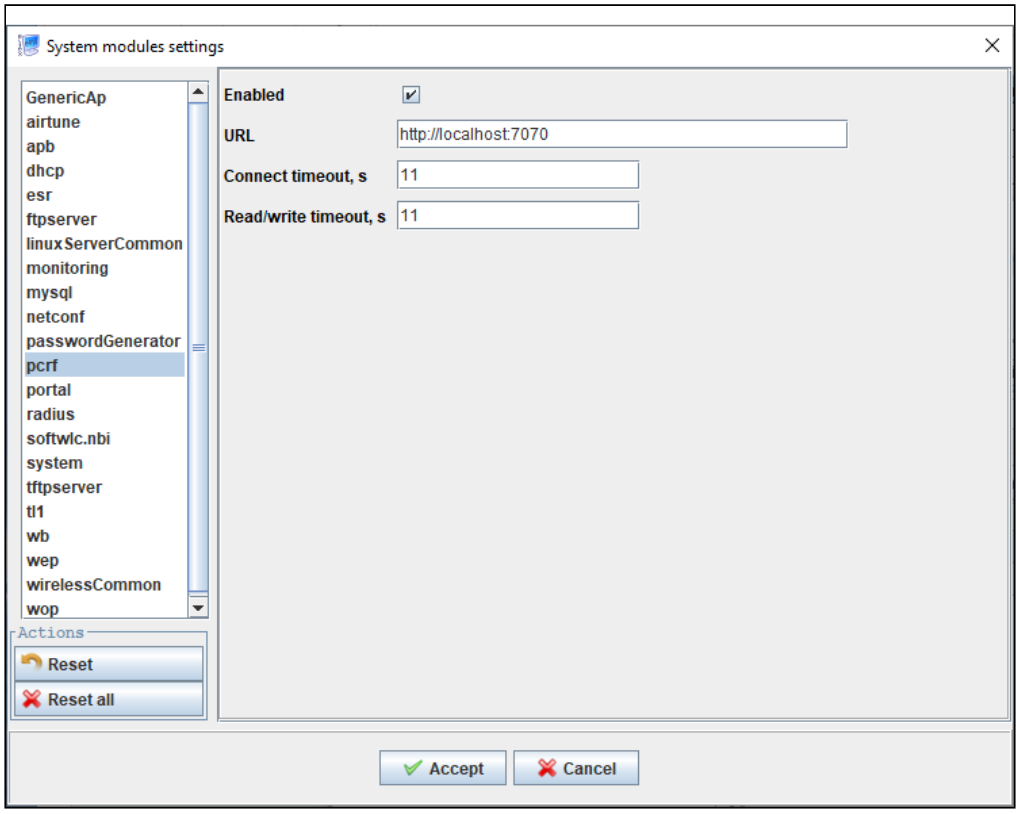



System settings → PCRF access

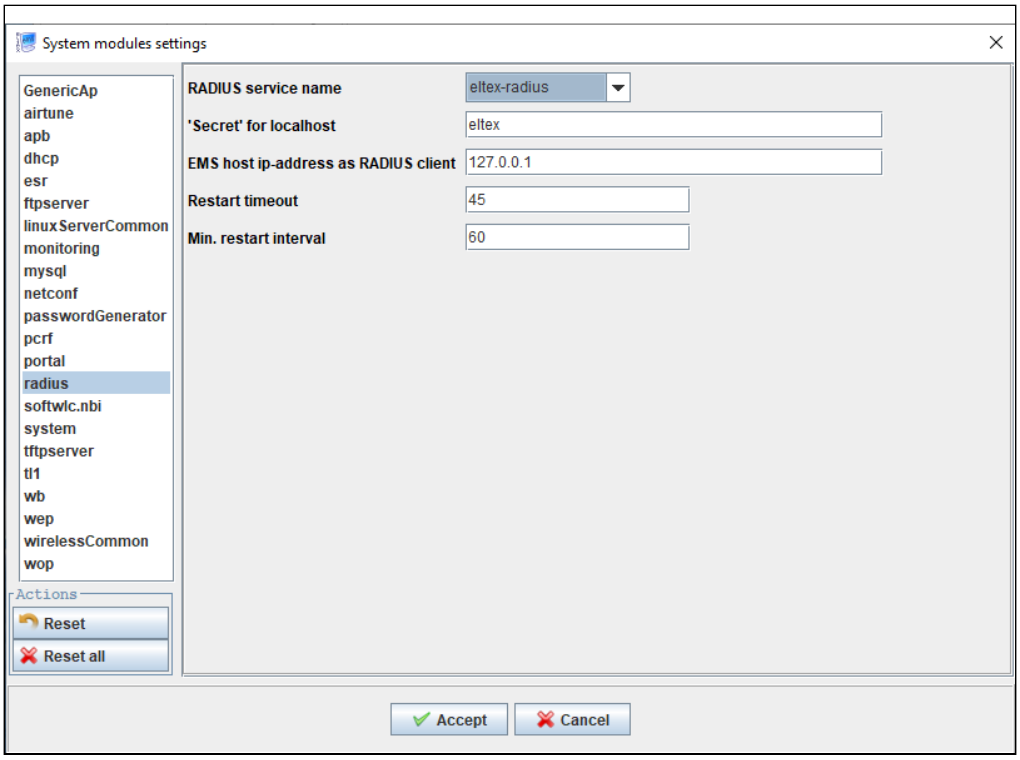


## EMS-GUI

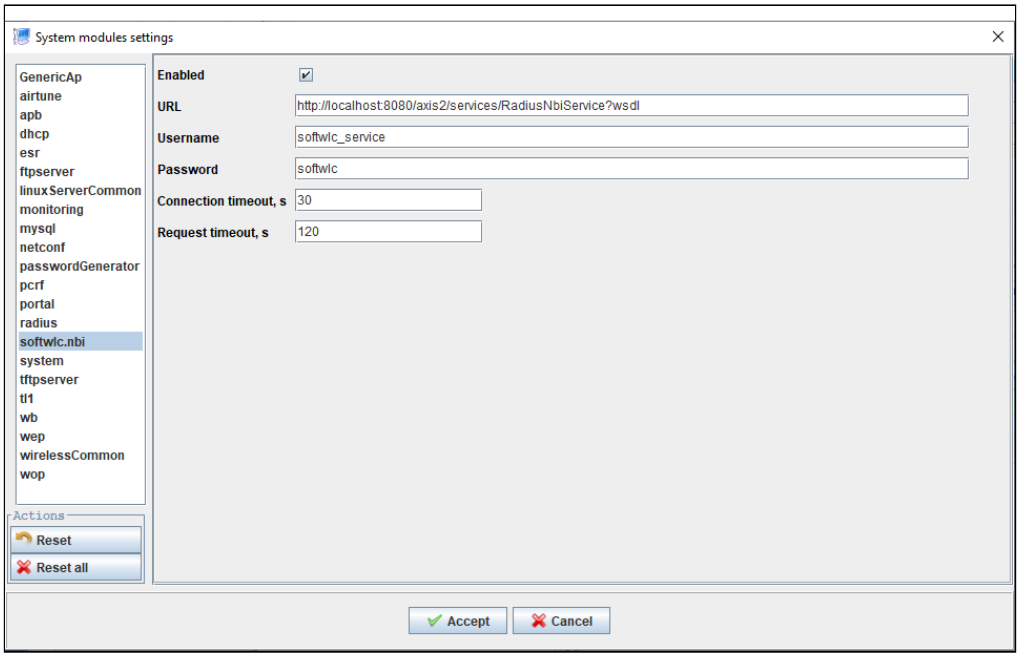
In EMS GUI, replace localhost (or 127.0.0.1) with a virtual IP address in the following sections:
Administration → EMS server configuration → System modules settings → pcrf



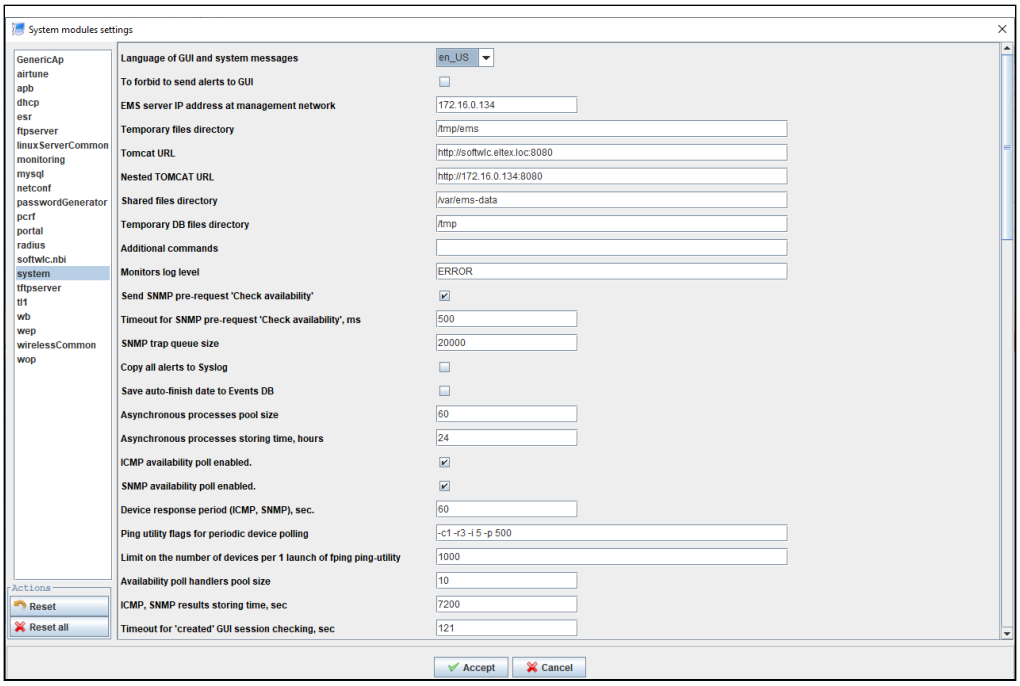

Administration → EMS server configuration → System modules settings → radius



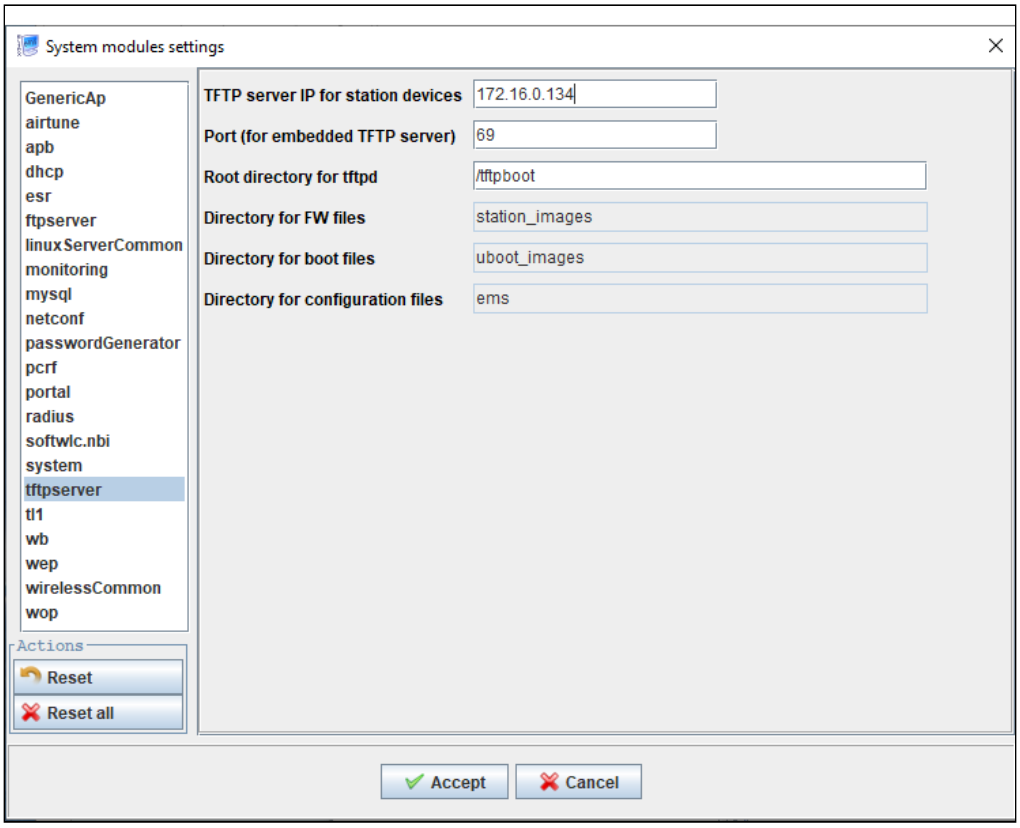

Administration → EMS server configuration → System modules settings → softwlc.nbi




Administration → EMS server configuration → System modules settings → system




Administration → EMS server configuration → System modules settings → tftpserver




## v1.14_keepalived_1.3.6 (EN)

- Package description
- Installation
- Starting/stopping procedure
- Configuration
    - Main configuration file
    - Test script
    - Role change configuration
    - Keepalived daemon configuration
- Saving a log to a separate file


> This manual is for **keepalived 1.3.6**
>
> As some critical functions are unstable in the version 1.2.15, the version 1.3.6 is recommended.

## Package description

keepalived package is an open source software used to perform high availability and load balancing functions. The first function is carried out by VRRP protocol implementation, and the second one is based on Linux Vitrual Server (IPVS). keepalived is not developed by Eltex and does not include any updates except configuration. A required version for the operating system used is compiled from source codes available in keepalived official repository on GitHub (https://github.com/acassen/keepalived). Keepalived is used for SoftWLC controllers backup organization, and only VRRP functionality is applied. Contact Wi-Fi or Broadband Access Service Center to get keepalived package for Ubuntu 14.04.

## Installation

To install the package, download it to a server and run the following command:

```
root@master:/# dpkg -i keepalived_1.3.6-eltexu14_amd64.deb
```

Installation should be carried out on behalf of root super user

## Starting/stopping procedure

To start the service, run the following command:

```
service keepalived start
```

If the service has been started successfully, the response will be:

```
keepalived start/running, process 2471
```

To stop the service:

```
root@master:/# service keepalived stop
```

System response:

```
keepalived stop/waiting
```

To check the service status, run the command:

```
root@master:/# service keepalived status
```

Response:

```
keepalived start/running, process 2809
```

### Configuration

keepalived configuration includes the next files:

| File | Description |
|---|---|
| /etc/keepalived/keepalived.conf | the main configuration file |
| /etc/keepalived/check_ping.sh | a script for EMS status check |
| /etc/keepalived/keep_notify.sh | a script ran on state change (when switching to MASTER, BACKUP, FAULT) |
| /etc/sysconfig/keepalived | keepalived launch parameters configuration file |
| /etc/keepalived/mongo_switch.js | a script for switching replicaSet MongoDB to the state relevant to VRRP |

#### Main configuration file

The listing of the main configuration file by default

**/etc/keepalived/keepalived.conf**

```
! Configuration File for keepalived

global_defs {
    notification_email {
       admin@example.org
    }
    notification_email_from softwlc@example.org
    smtp_server mail.example.org
    smtp_connect_timeout 30
    router_id swlc1
    enable_traps
}

vrrp_script check_network {
    script "/etc/keepalived/check_ping.sh"
    interval 5
    weight 50
    fall 3
    rise 3
    init_fail
    user root
}

vrrp_instance VI_SWLC {
    state BACKUP
    interface eth0
    virtual_router_id 1
    track_script {
        check_network
    }
    track_interface {
        eth0 weight 50
    }
    priority 150
    advert_int 1
    nopreempt
    authentication {
        auth_type PASS
        auth_pass eltex
    }
    virtual_ipaddress {
        <virtual_ip> dev eth0 label eth0:1
    }

    notify_master "/etc/keepalived/keep_notify.sh master"
    notify_backup "/etc/keepalived/keep_notify.sh backup"
    notify_fault "/etc/keepalived/keep_notify.sh fault"

```

```
    unicast_peer {
        <ip_server1>
    }
}
```

The configuration file consists of three main sections: **global_defs, vrrp_script, vrrp_instance.** The first and the second sections contain definitions of global parameters and the state checking script's configuration respectively, and the third one describes the VRRP instance itself.

### Test script

The current implementation offers the following script as a test one:

**/etc/keepalived/check_ping.sh**

```
#!/bin/bash

# host to ping
# there - default gw
HOST=<default_gw_ip>
# -q quiet
# -c nb of pings to perform
ping -q -c5 $HOST > /dev/null

# $? var keeping result of execution
# previous command
if [ $? -eq 0 ]
    then
        echo `date +"%T %F"` "OK gw reachable"
        EXIT_CODE=0
    else
        echo `date +"%T %F"` "ERROR gw unreacheble!"
        EXIT_CODE=1
fi

exit $EXIT_CODE
```

the script pings a default gateway and returns an output code. Thus, SoftWLC is guaranteed to be accessible for external clients if the script has been executed successfully.

### Role change configuration

When the server's state is changed, the keep_notify.sh script is started.

**/etc/keepalived/keep_notify.sh**

```
#!/bin/bash

MYSQL_USER="<mysql_user>"
MYSQL_PASSWORD="<mysql_password>"

mongo_set_role() {
    local role="$1"
    if [[ "$(which mongo)" ]]; then
        mongo --quiet --eval "var role=\"$role\"" admin /etc/keepalived/mongo_switch.js
        # Uncomment if using mongodb auth
        #mongo -u<username> -p<password> --quiet --eval "var role=\"$role\"" admin /etc/
keepalived/mongo_switch.js
    fi
}

if ! lockfile-create --use-pid -r 5 /tmp/keep.mode.lock; then
    echo "Unable to lock"
    echo "Unable to lock" > /tmp/keep.mode.lock.fail
    exit 0
fi

case "$1" in
    master)
    #  ems_reload_all
    echo "MASTER" > /tmp/keep.mode

    mongo_set_role master
    service eltex-ems restart
    service tomcat7 restart
    service eltex-ngw restart

    # рестарт слейва MySQL чтобы при восстановлении связи - сразу получить изменения,
    # а не ждать периодического heartbeat от второго сервера
    mysql -u$MYSQL_USER -p$MYSQL_PASSWORD -e "stop slave"
    mysql -u$MYSQL_USER -p$MYSQL_PASSWORD -e "start slave"
  ;;
 backup)
    echo "BACKUP" > /tmp/keep.mode
    mongo_set_role slave
    service mongodb restart
    service eltex-ems stop
    service tomcat7 stop
    service eltex-ngw stop
    mysql -u$MYSQL_USER -p$MYSQL_PASSWORD -e "stop slave"
    mysql -u$MYSQL_USER -p$MYSQL_PASSWORD -e "start slave"
 ;;
 fault)
    echo "FAULT" > /tmp/keep.mode
```

```
    mongo_set_role slave
    service mongodb restart
 ;;
 *)
    echo "Usage: $0 {master|backup|fault}"
    exit 1
esac

lockfile-remove /tmp/keep.mode.lock;

exit 0
```

ReplicaSet MongoDB master changing script.

**/etc/keepalived/mongo_switch.js**

```
// Provided by environment
var role;

if (role != 'master' && role != 'slave') {
    throw "Role must be either master or slave";
}

var thisIsMaster = (role == 'master');
var status = rs.isMaster();
var thisHost = status.me;

print("Primary: " + status.ismaster + "; applying configuration ...");
var cfg = rs.conf();
for (var i = 0; i < cfg.members.length; i++) {
    var member = cfg.members[i];
    var self = (member.host == thisHost);
    if (self ^ thisIsMaster) {
        // Configuration for slave
        member.priority = 1;
        member.votes = 0;

        print(member.host + ": secondary");
    } else {
        // Configuration for master
        member.priority = 2;
        member.votes = 1;

        print(member.host + ": primary");
    }
}

var result = rs.reconfig(cfg, { force: !status.ismaster });
if (result.ok == 1) {
    print("Reconfiguration done");
} else {
    print(result);
}
```

Keepalived daemon configuration

Parameters for launching etc.

### Saving a log to a separate file

By default, **keepalived** writes a log to the **/var/log/syslog** file. For keepalived debugging, monitoring and managing convenience, separate log filing can be configured. **rsyslog** configuration example is introduced below:

```
nano -w /etc/rsyslog.d/10-keepalived.conf
if $programname contains 'Keepalived' then /var/log/keepalived.log
if $programname contains 'Keepalived' then ~
```

Then restart rsyslog using the command:

```
root@swlc01-server:/# service rsyslog restart
```

Messages from keepalived daemon will be written only to the **/var/log/keepalived.log** file, not to the **/var/log/syslog**.

## v1.14_Configuring SSID password change report sending (EN)

1. The instruction on creating tasks for automatic change of SSID passwords is available here: Instruction
2. To send a report, correct parameters of alert messages sending via E-mail should be set in "system" module of EMS.

**Activating SSID password change notification**

- The functionality is activated via EMS GUI, section "Administration" → ''EMS server configuration" → ''System modules" → ''wirelessCommon". Settings are described at the separate section "SSID password notifier settings".Several e-mail addresses can be entered, separated by ";".

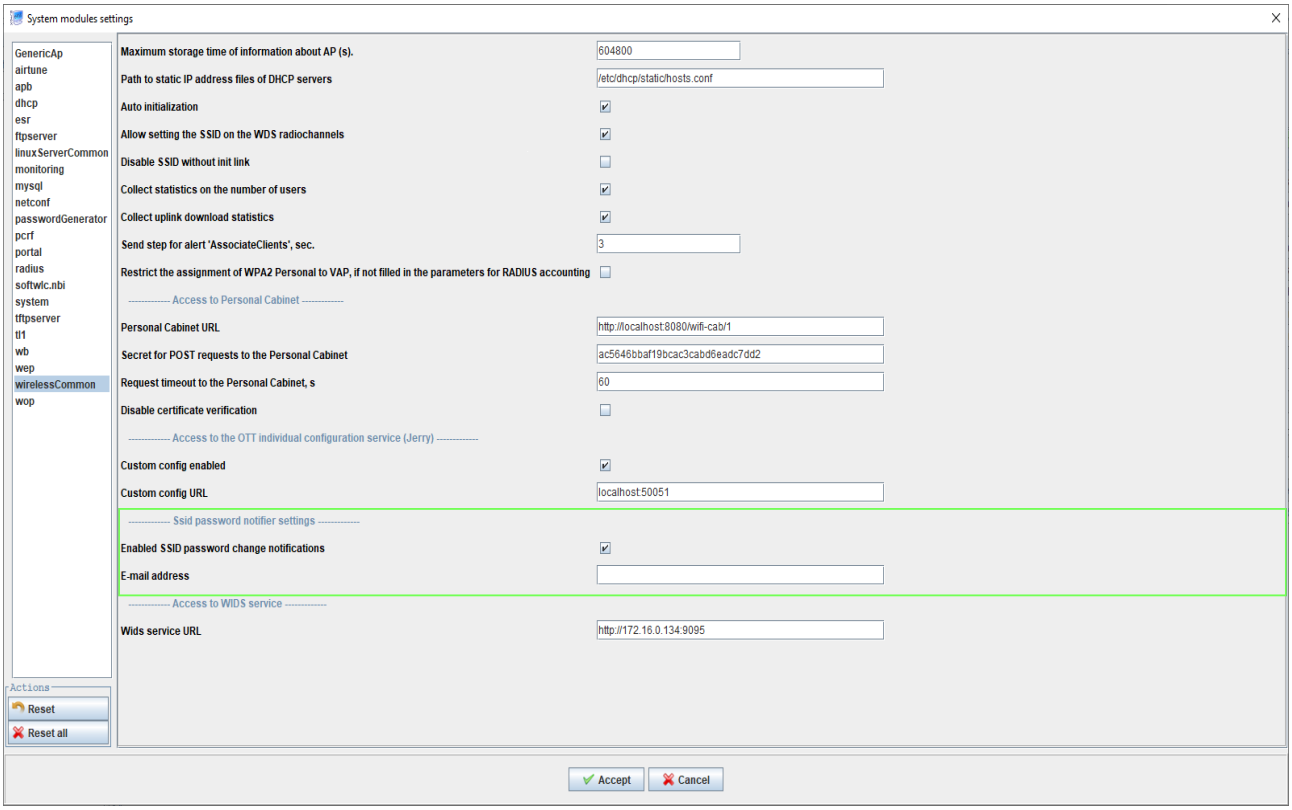



**Figure 1** — EMS scheduled SSID password change notifications settings

- SSID password change report is sent in accordance with the "Monitor for sending scheduled SSID password change report" operation. The monitor can be set both for single (manual) and period sending (by CRON period). The report contains data about last password changes (SSID identifiers of networks with changed passwords, the number of access points with these SSIDs, SSID password change task errors indicating access points and task ID in EMS).

For the report to be appropriate, the monitor should be started some time after SSID password change tasks. Otherwise, SSID password change tasks will be completed after report sending, and data will be incorrect. It is recommended to start "Monitor for sending scheduled SSID password change report" 30-60 minutes after running scheduled SSID password change tasks.

## v1.14_Integration with HotWiFi (EN)

- Access point firmware
- Setting up connection between the advertising platform and an access point
- Setting up connection between the advertising platform and BRAS

## Access point firmware

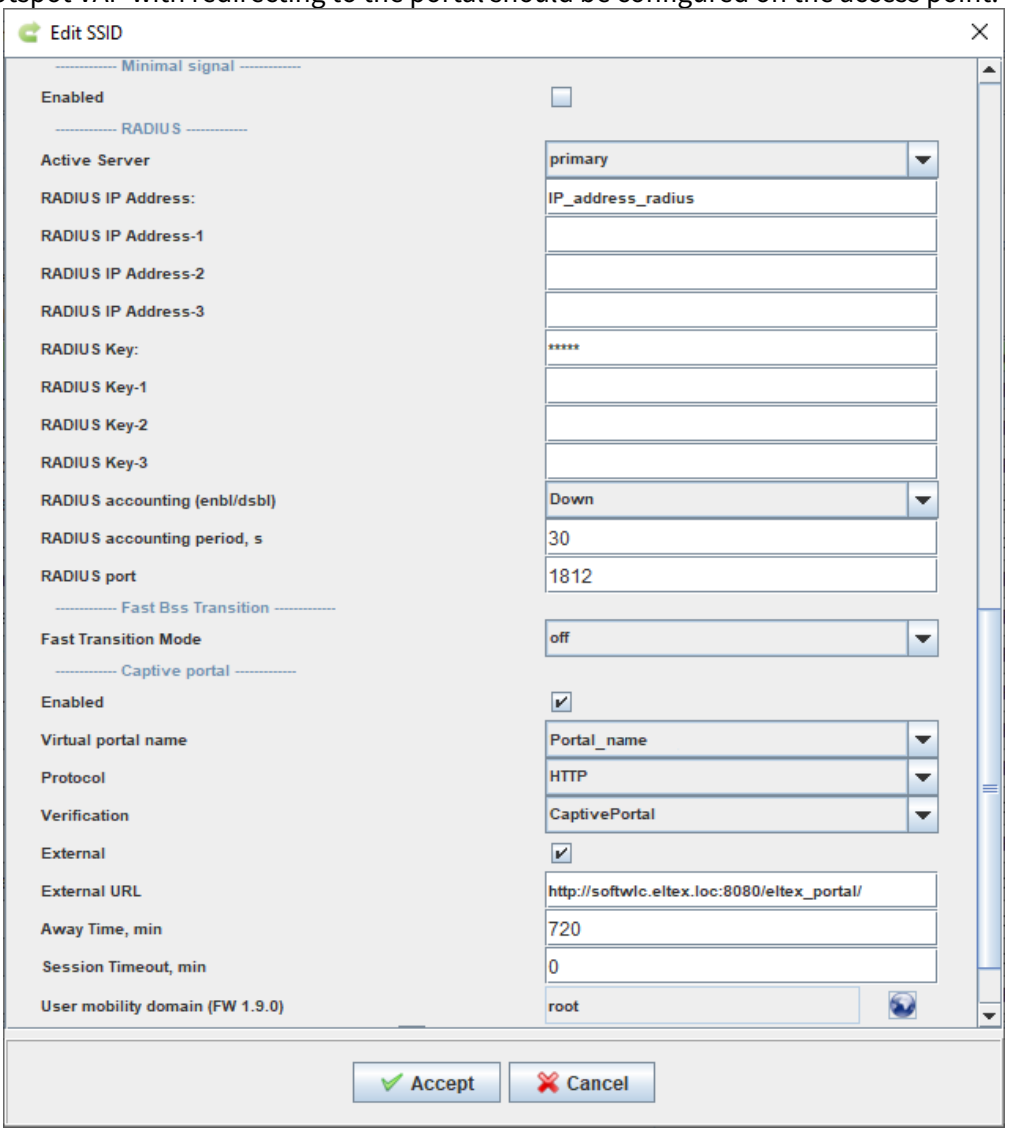
To test integration with Hot-WiFi advertising platform, firmware version 1.11.0.47 or higher is needed.

Download link:

https://eltex-co.com/support/

## Setting up connection between the advertising platform and an access point

1. A test hotspot VAP with redirecting to the portal should be configured on the access point:



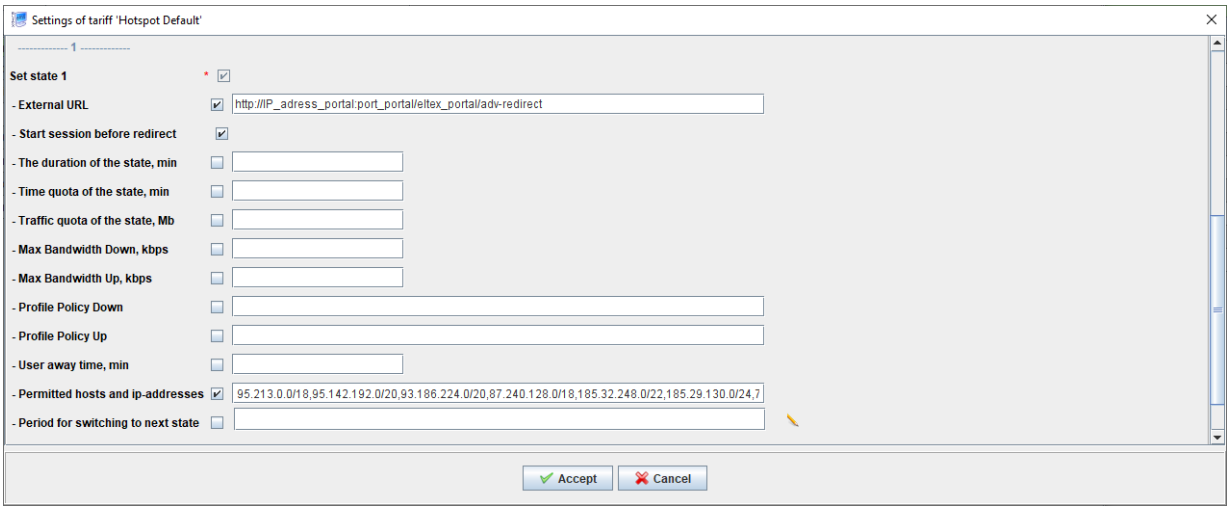

2. Create an advertising tariff. The first scenario should be an external URL address in the following form: http://<portal-ip-address>:<portal_port>/eltex_portal/adv-redirect. The addresses should be added to the list of permitted hosts for this scenario. Any further scenarios can be defined in a

standard form (for example, 1-minute internet access as the second scenario, a return to a portal and client reauthorization as the third scenario).

⚠ In order to provide correct operation, two or more scenarios should be created for one tariff.

### The list of permitted hosts

95.213.0.0/18,95.142.192.0/20,93.186.224.0/20,87.240.128.0/18,185.32.248.0/22,185.29.130.0/24,74.119.76.0/22,69.63.176.0/20,69.171.224.0/19,66.220.144.0/20,45.64.40.0/22,103.4.96.0/22,31.13.64.0/18,31.13.24.0/21,204.15.20.0/22,199.201.64.0/22,173.252.64.0/18,157.240.0.0/16,8.25.197.0/24,8.25.196.0/24,8.25.195.0/24,199.96.56.0/21,199.16.156.0/22,192.133.76.0/22,185.45.4.0/22,104.244.40.0/21,5.61.16.0/21,217.20.144.0/20,185.16.244.0/22,54.144.0.0/12,54.160.0.0/12,52.0.0.0/11,54.208.0.0/13,54.216.0.
0/14,54.220.0.0/15,107.20.0.0/14,31.13.93.0/24,212.30.134.0/24,173.194.0.0/16,64.233.160.0/19,184.84.0.0/14,104.108.32.0/20,199.59.148.0/22,2.21.7.26,188.166.114.145,46.101.169.141,217.69.128.0/20,api.instagram.com,instagram.com,instagram.c10r.facebook.com,www.instagram.com,static.licdn.com,platform.linkedin.com,ssl.gstatic.com,cp.hot-wifi.ru,www.linkedin.com,mc.yandex.ru,cdn.hot-wifi.ru,www.facebook.com,facebook.com,185.60.216.0/24,74.125.0.0/16,auth-pro.wifi.rt.ru,
78.155.202.186

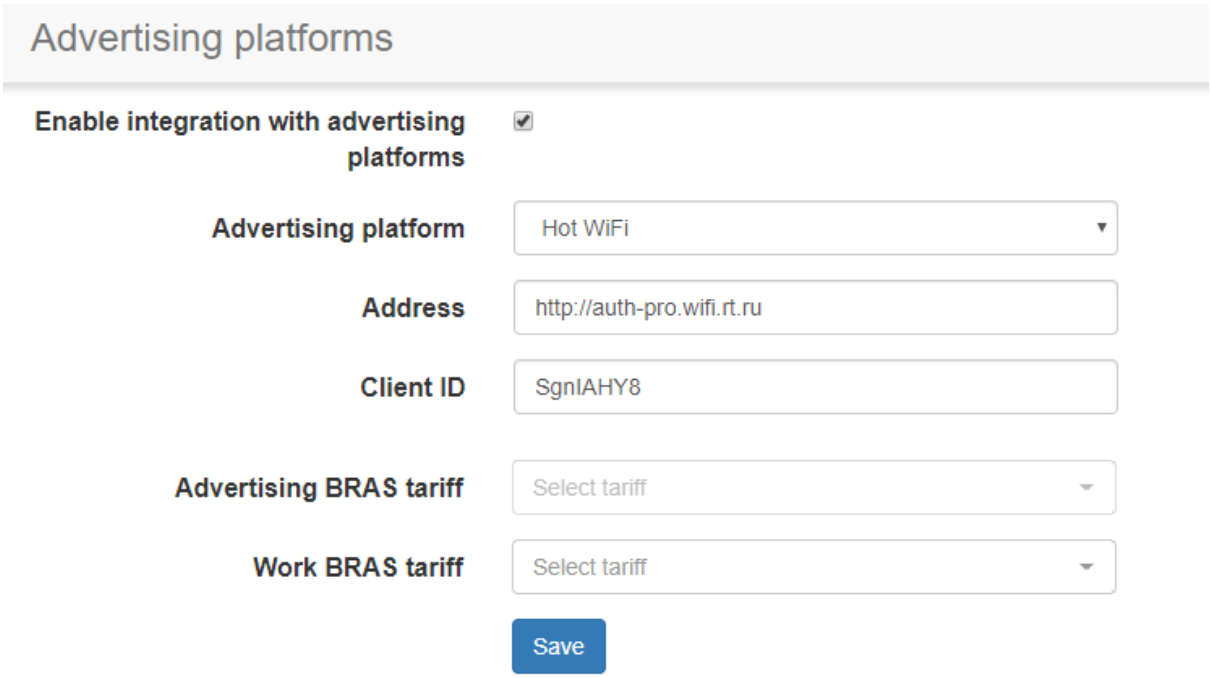



3. Go to the *Portal Constructor*, choose a portal used for testing. In the "Tariffs" section of the menu, choose the tariff created for testing, enter its name and save changes.

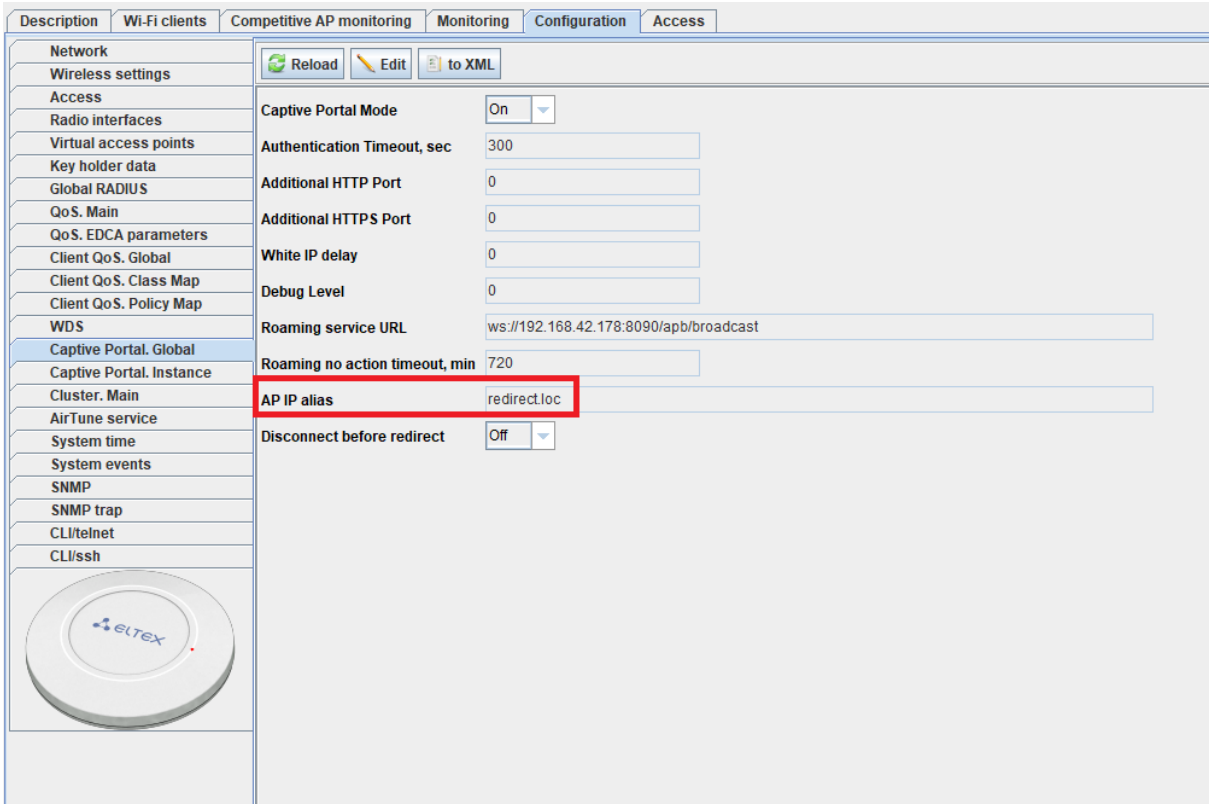
4. Go to the "Advertising platforms" section, enable integration and choose Hot-WiFi advertising platform. Address: http://auth-pro.wifi.rt.ru, client ID: `SgnlAHY8`, save changes.

The tariffs selected here are valid only for BRAS, tariffs for native access points should be selected in "Tariffs" tab.

If BRAS is not used, leave "Advertising BRAS tariff" and "BRAS tariff after advertising" fields blank.




5. Make sure that AP IP Alias is defined on each access point within a domain




The parameter should be the same for all the access points of the platform. Configuration can be done directly on the access point, via group operations or using an access point initialization rule.

6. For Hot-WiFi integration, Hot-WiFi API service access from SoftWLC core is needed. A check is performed by Eltex-Portal module. If it is completed successfully, you will be redirected to Hot-WiFi platform, otherwise you will be redirected to a website defined in "Redirection URL" field of "Language settings" section.
To check URL, curl utility can be used
Example:

```
tester@tester:~$ curl http://auth-pro.wifi.rt.ru/_info
{
  "status": "OK"
}
tester@tester:~$
```

7. Make sure that a registered client is redirected to an advertising platform website and successfully logs on to social networks and sees advertising banners.

## Setting up connection between the advertising platform and BRAS

To configure integration with Hot-WiFi, the following steps should be performed:

1. Log in to the Personal Cabinet
2. Go to "Settings" → "URL lists" and create "hot-wifi" URL list.

The list should contain the portal address and URL for correct AndroidConnectivityManager operation. It should also contain Hot-WiFi advertising platform templates

### List example

URL:
http://192.168.107.213:8080/eltex_portal/
http://connectivitycheck.gstatic.com/generate_204/
https://connectivitycheck.gstatic.com/generate_204/

Шаблоны:

^((https|http):\/\/)(.+\.)?abs\.twimg\.com

^((https|http):\/\/)(.+\.)?accounts\.google\.com

^((https|http):\/\/)(.+\.)?api\.instagram\.com

^((https|http):\/\/)(.+\.)?apple\.com

^((https|http):\/\/)(.+\.)?captive\.apple\.com

^((https|http):\/\/)(.+\.)?facebook\.com

^((https|http):\/\/)(.+\.)?facebook\.net

^((https|http):\/\/)(.+\.)?fbcdn\.net

^((https|http):\/\/)(.+\.)?fbstatic-a\.akamaihd\.net

^((https|http):\/\/)(.+\.)?googleapis\.com

^((https|http):\/\/)(.+\.)?googleusercontent\.com

^((https|http):\/\/)(.+\.)?hot-wifi\.ru

^((https|http):\/\/)(.+\.)?inkedin\.com

^((https|http):\/\/)(.+\.)?instagram\.c10r\.facebook\.com

^((https|http):\/\/)(.+\.)?instagram\\.com

^((https|http):\/\/)(.+\.)?licdn\.com

^((https|http):\/\/)(.+\.)?oauth\.vk\.com

^((https|http):\/\/)(.+\.)?odnoklassniki\.ru

^((https|http):\/\/)(.+\.)?ok\.ru

^((https|http):\/\/)(.+\.)?top-fwz1\.mail\.ru

^((https|http):\/\/)(.+\.)?twimg\.com

^((https|http):\/\/)(.+\.)?twitter\.com

^((https|http):\/\/)(.+\.)?userapi\.com

^((https|http):\/\/)(.+\.)?userapi\\.com

^((https|http):\/\/)(.+\.)?vk\.com

^((https|http):\/\/)(.+\.)?vk\.me

^((https|http):\/\/)(.+\.)?wifiworld\.me

^((https|http):\/\/)(.+\.)?www\.instagram\.com

^((https|http):\/\/)(.+\.)gosuslugi\.ru

^((https|http):\/\/)api\.instagram\.com

^((https|http):\/\/)auth-pro\.wifi\.rt\.ru

^((https|http):\/\/)cdn\.hot-wifi\.ru

^((https|http):\/\/)cp\.hot-wifi\.ru

^((https|http):\/\/)fbstatic-a\.akamaihd\.net

^((https|http):\/\/)instagram\.c10r\.facebook\.commail

^((https|http):\/\/)instagram\.com

^((https|http):\/\/)mc\.yandex\.ru

^((https|http):\/\/)platform\.linkedin\.com

^((https|http):\/\/)ssl\.gstatic\.com

^((https|http):\/\/)static\.licdn\.com

^((https|http):\/\/)www\.instagram\.com

^((https|http):\/\/)www\.linkedin\.com

An updated list can be found on http://be.hot-wifi.ru/api/walledgarden/get, but it should be changed in accordance with the example above to be downloaded properly.

3. Go to "Services and tariffs" → "PCRF services" and create a service HOTWIFI (any name)

   Traffic's class: WELCOME (The name should be the same as for traffic class in ESR-1000 configuration)

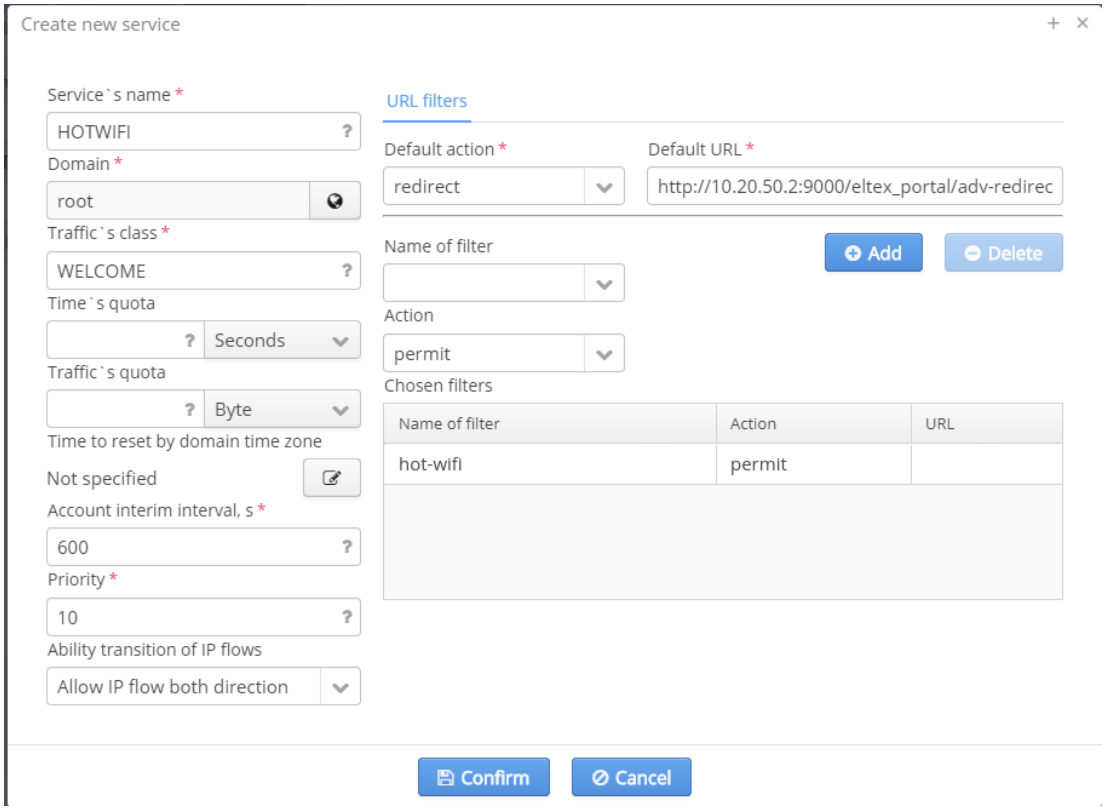
   Default action: redirect

   Default URL: http://<portal-ip-address>:<portal_port>/eltex_portal/adv-redirect

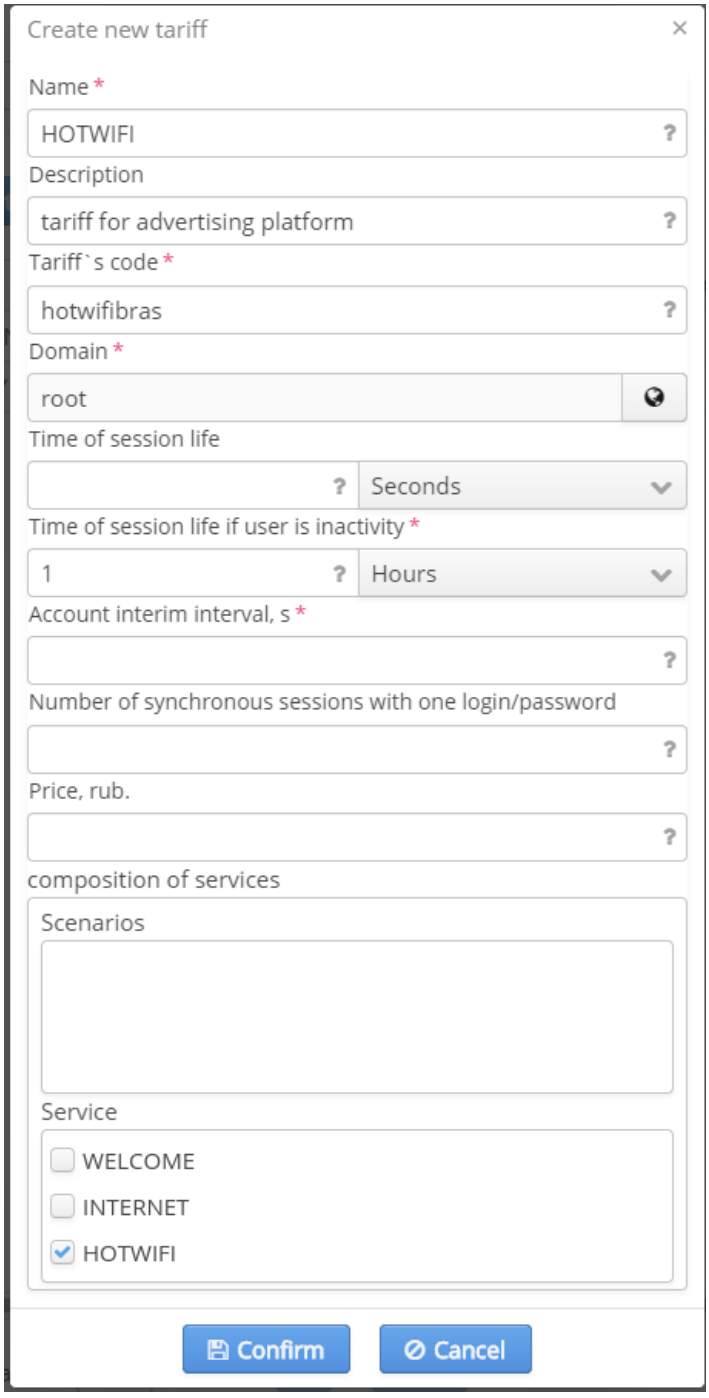
   Filter

   Action: permit

   Name of filter: hot-wifi




4. Go to "Services and tariffs" → "Tariffs", select a PCRF/BRAS filter, create HOTWIFI tariff with hotwifi service




5. Go to the Portal Constructor

6. Create a portal, go to "Advertising platforms" and check "Enable integration" box

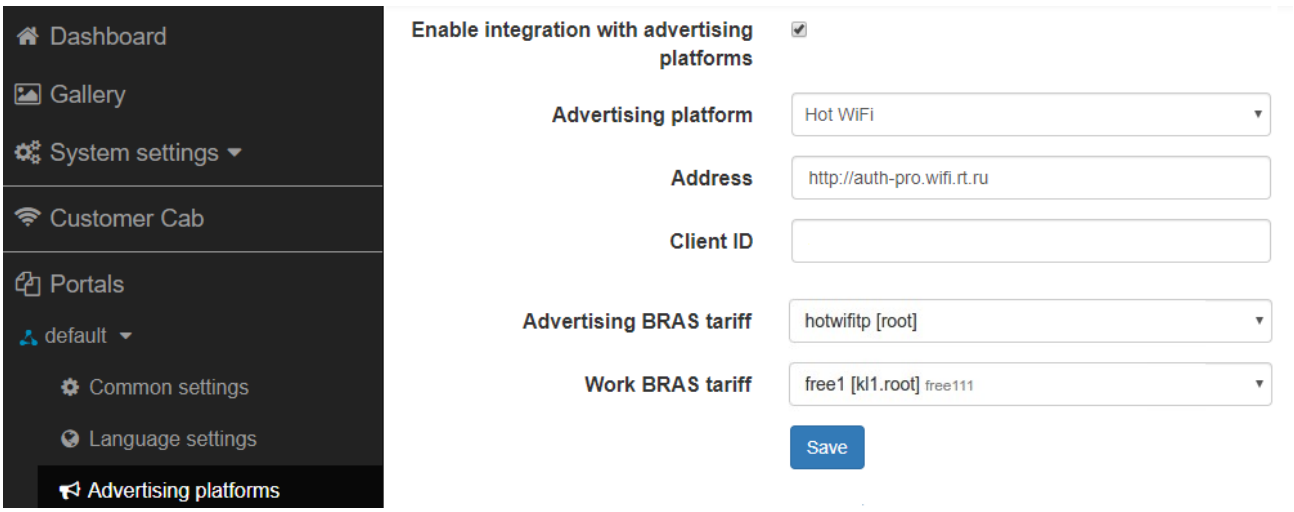
7. Select Hot-WiFi advertising platform, fill in the fields

   Address:  an address in the following form: http://auth-pro.wifi.rt.ru, which is provided by Hot-WiFi staff

   Client ID: client identifier provided by Hot-WiFi staff

   Advertising BRAS tariff:  select the tariff created in paragraph 4

BRAS tariff after advertising: any tariff

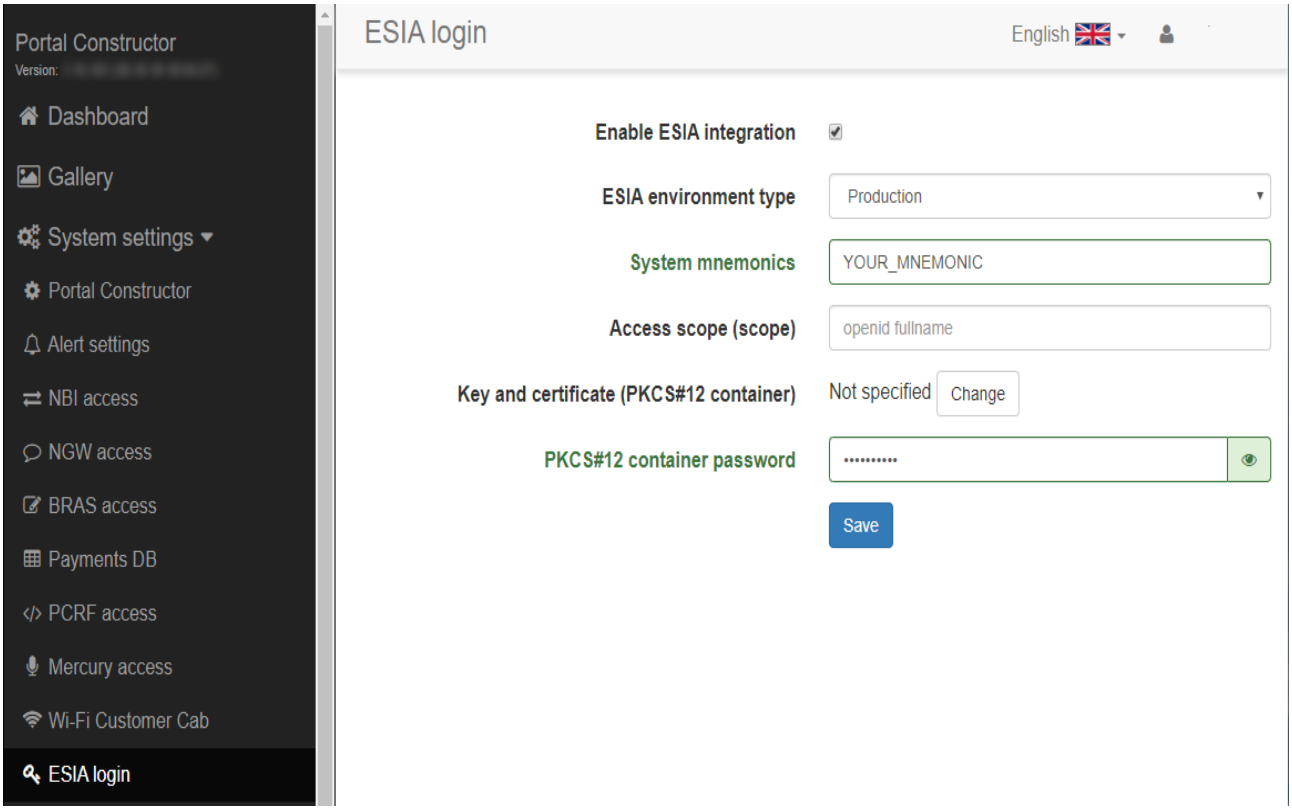



If an advertising platform is enabled, the tariffs selected in "Advertising platforms" are used, other tariffs will be ignored.

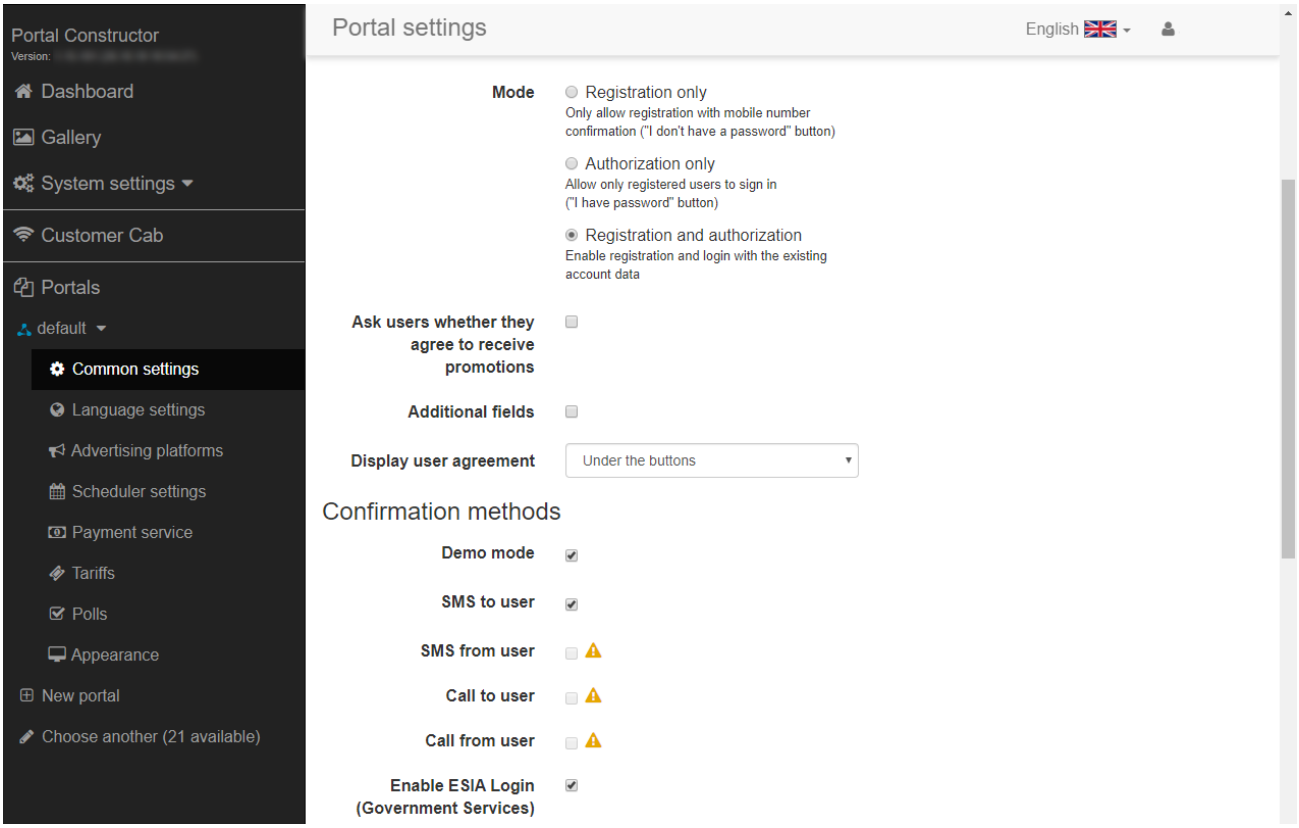
## v1.14_Integration with ESIA (EN)

Enable integration via "ESIA login" section of the Portal Constructor and set the required parameters

- ESIA environment type. Both environment types require information system registration in the Ministry of Digital Development, Communications and Mass Media
- System mnemonics (identifier). Should be consistent with the one specified in the application for ESIA connection
- Access scope (scope). Should be consistent with ones specified in the application. At least a fullname should be specified for correct operation
- Key and certificate. Download PKCS#12 (.p12 or .pfx) container with the relevant key and the certificate specified in the application for ESIA connection
- PKCS#12 container password




Enable ESIA login in Common settings.




Whitelist the following domains on APB:

- **esia-portal1.test.gosuslugi.ru** - for test environment
- **esia.gosuslugi.ru** - for production environment

Whitelists are configured in **/etc/eltex-apb/hosts.json.**

```
[{"permitted-ip-list": [
"^esia-portal1\\.test\\.gosuslugi\\.ru$",
"^esia\\.gosuslugi\\.ru$",]
}]
```

Provide an opportunity for access points to resolve domain names. For this purpose:

- Configure DNS server that is accessible from AP management network
- Configure DNS server address sending to access points on DHCP

ⓘ An access point should resolve the domains above correctly, while access to them (to the internet) is not necessary.

Provide access to ESIA servers from Captive Portal authorization server

## v1.14_Using TLS certificates for user authorization (EN)


- 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:./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:

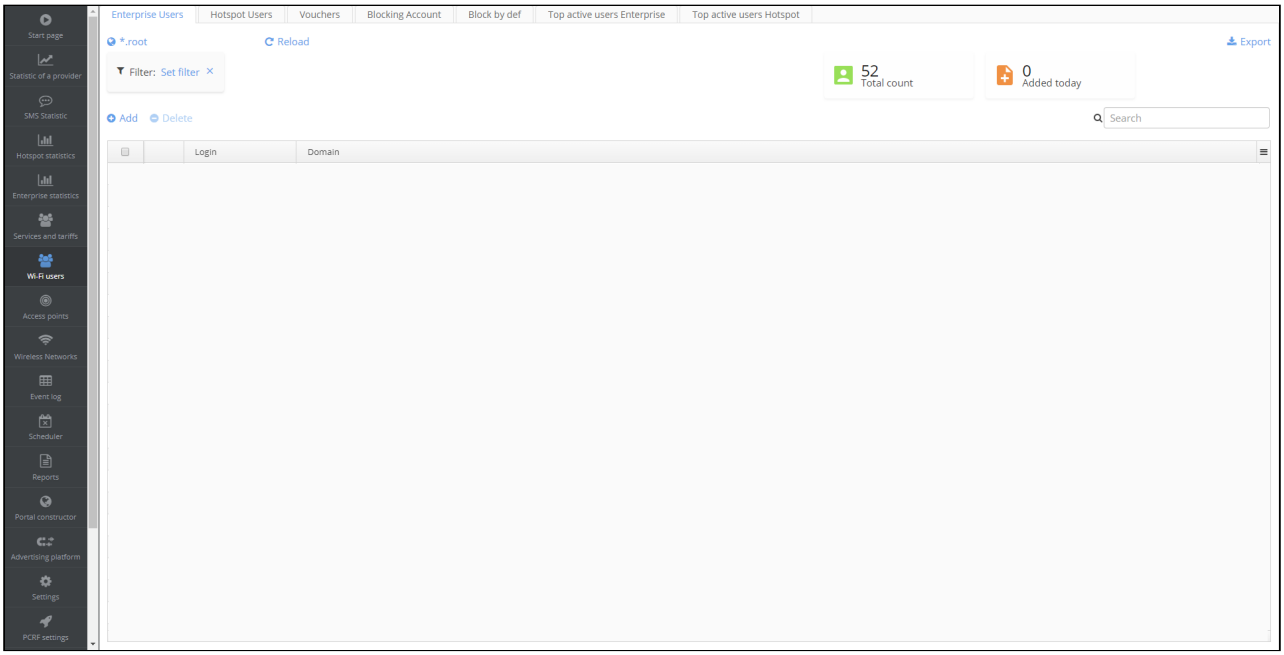
1. Open the file **cat /etc/eltex-radius-nbi/radius_nbi_config.txt** and specify an address that is referred by a user to request the Admin Panel (127.0.0.1 by default).

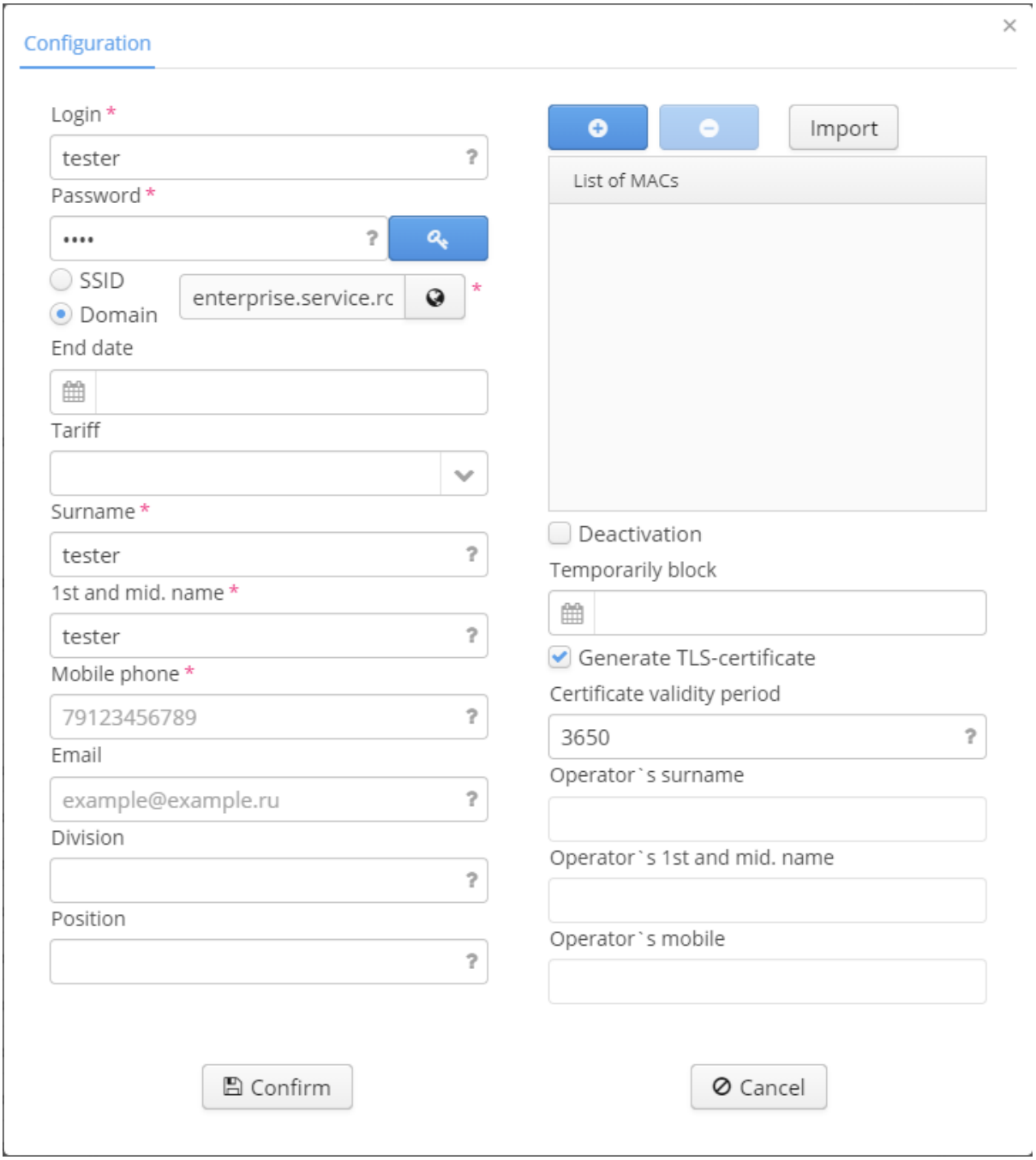
   # tomcat url

   tomcat.host=127.0.0.1

   tomcat.port=8080

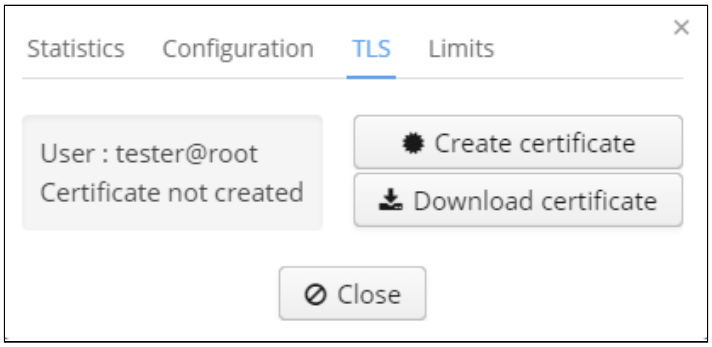
2. Enter the Admin Panel and open the tab "Wi-Fi Users" -> "Enterprise users". Click "Add".


Start page
Statistic of a provider
SMS Statistic
Hotspot statistics
Enterprise statistics
Services and tariffs
Wi-Fi users
Access points
Wireless Networks
Event log
Scheduler
Reports
Portal constructor
Advertising platform
Settings
PCRF settings
Enterprise Users
Hotspot Users
Vouchers
Blocking Account
Block by def
Top active users Enterprise
Top active users Hotspot
*.root
Reload
Export
Filter: Set filter
52
Total count
0
Added today
Add
Delete
Search
Login
Domain




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

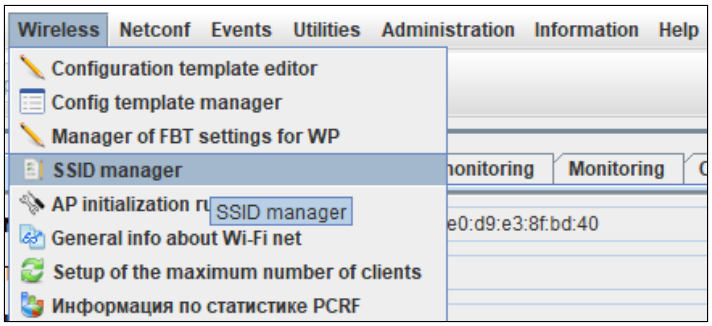
By default, a certificate is valid for 3650 days. Change this parameter if necessary.

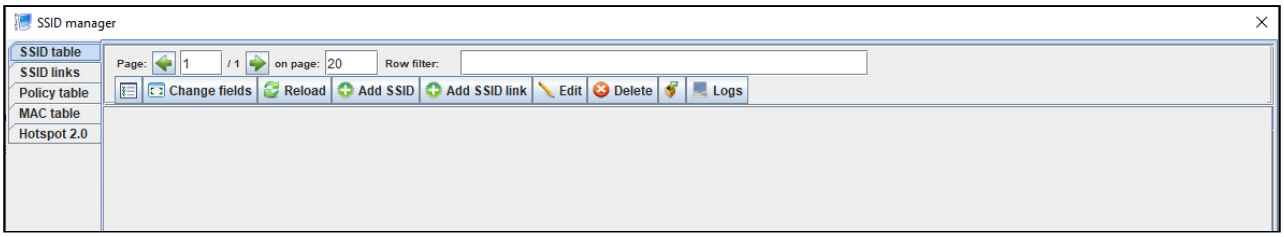



After a user is created, his parameters can be seen. Check the tab "TLS" to verify a certificate has been generated.

## 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`

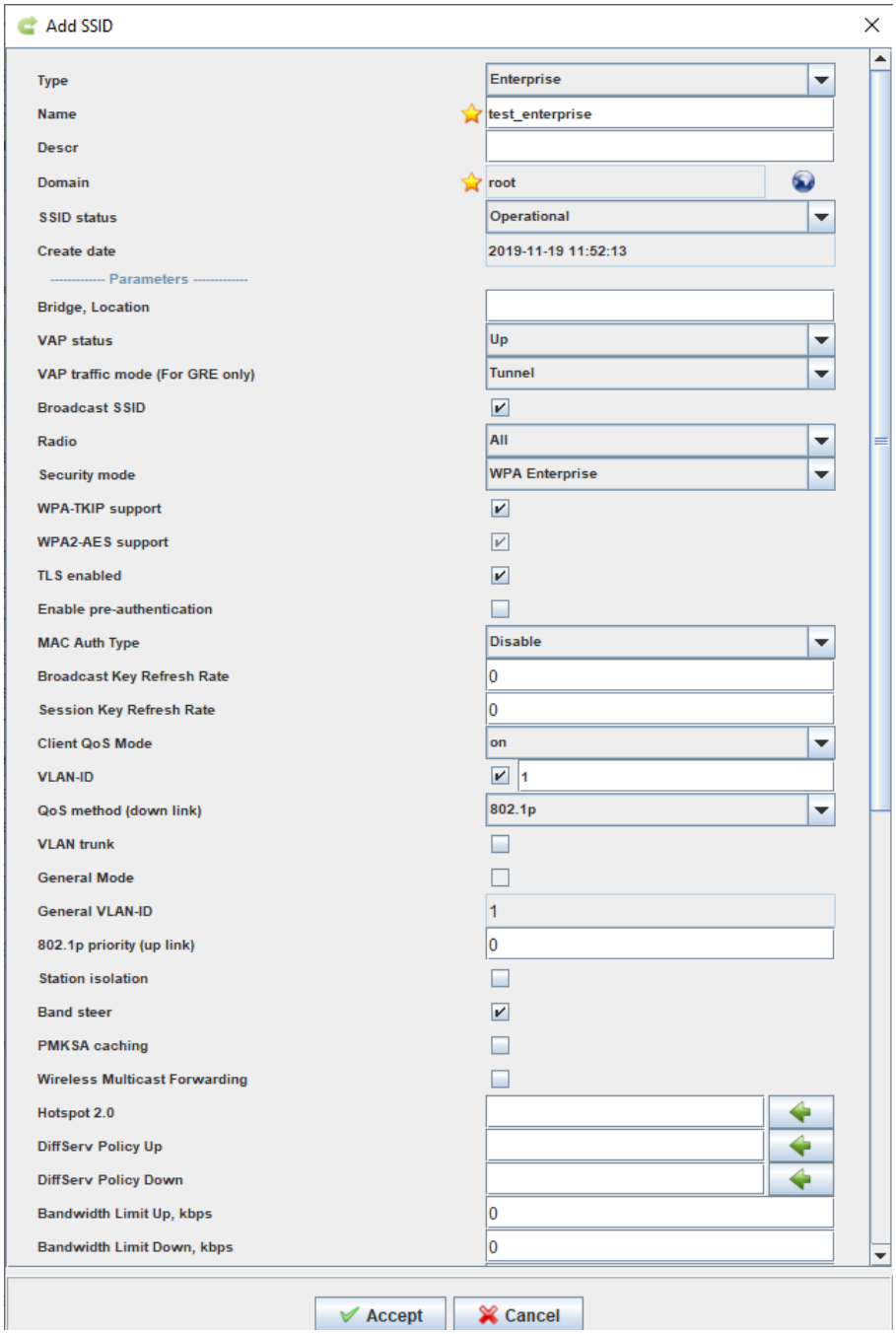
```
RADIUS accounting – up

RADIUS accounting period – 600
```

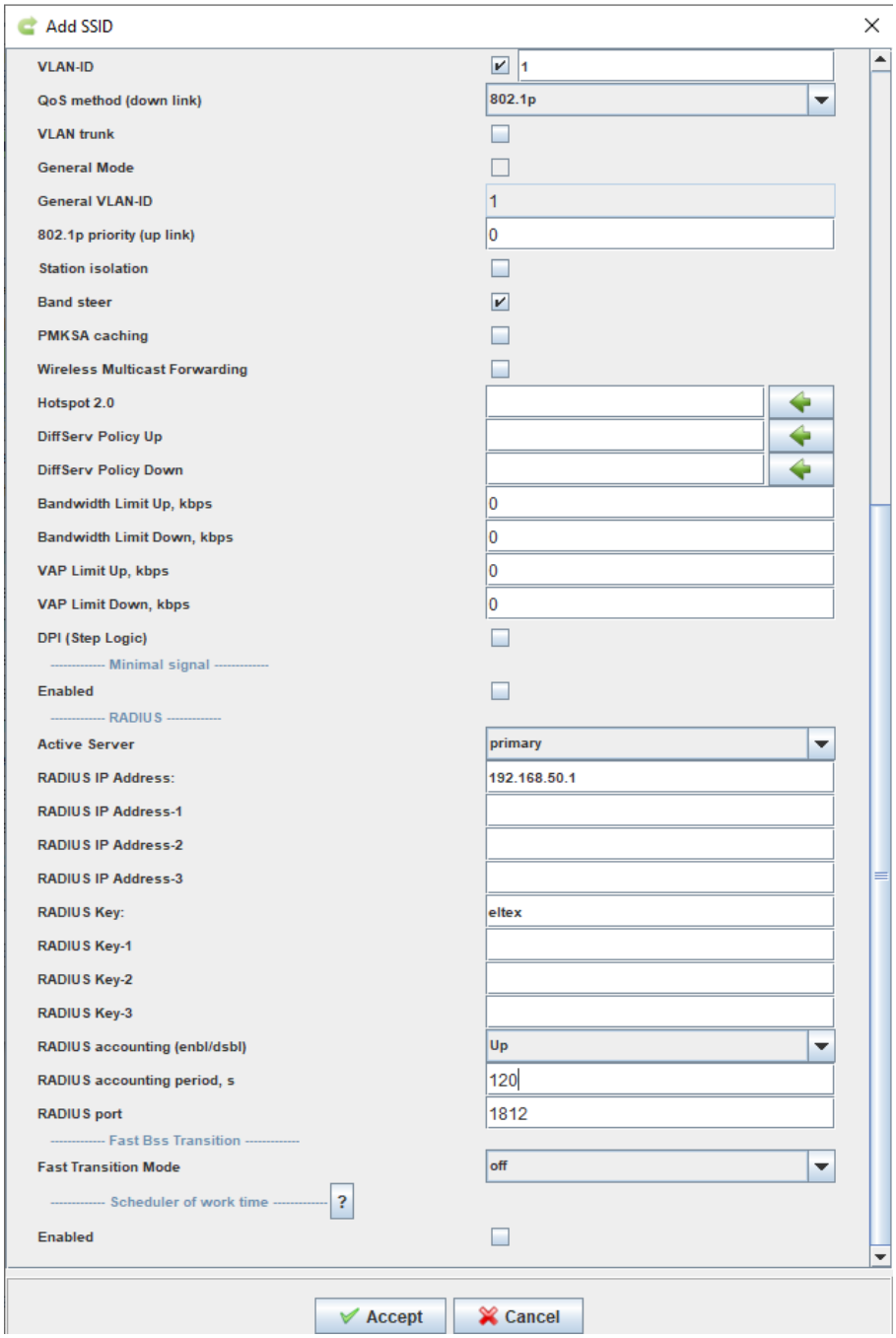
Select radio interfaces to which a created SSID will be assigned.

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'.*

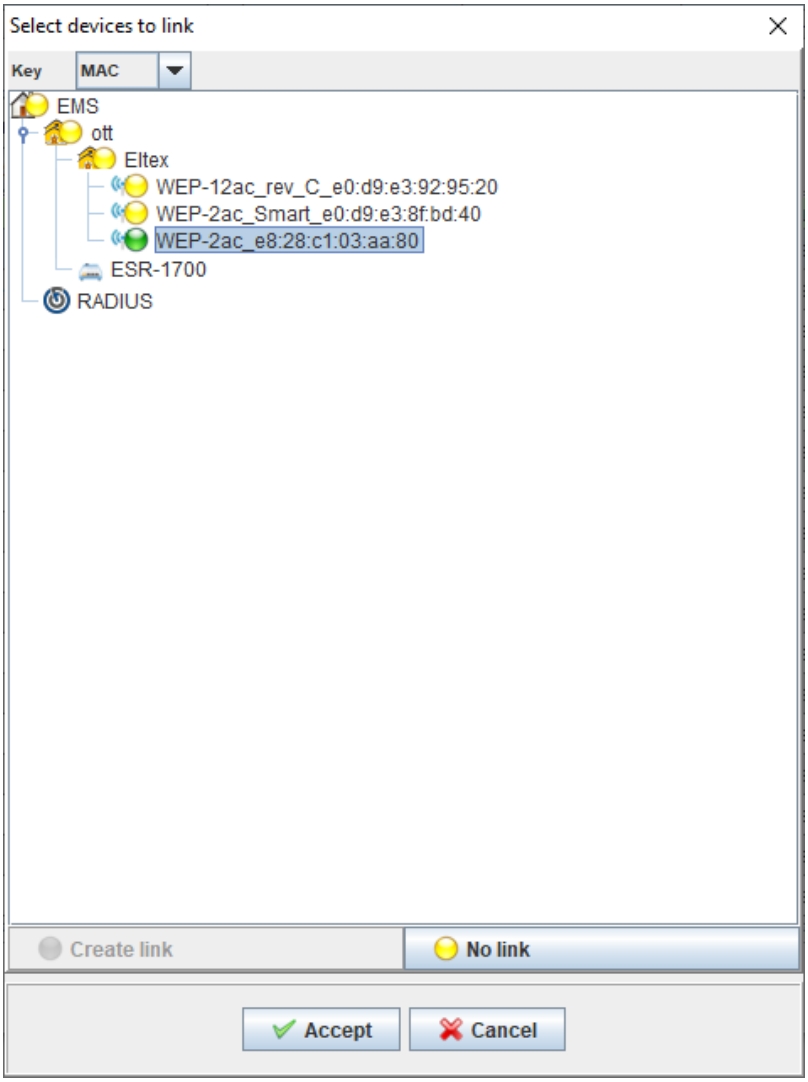

Add SSID
Type
Enterprise
Name
test_enterprise
Descr
Domain
root
SSID status
Operational
Create date
2019-11-19 11:52:13
---------- Parameters ----------
Bridge, Location
VAP status
Up
VAP traffic mode (For GRE only)
Tunnel
Broadcast SSID
Radio
All
Security mode
WPA Enterprise
WPA-TKIP support
WPA2-AES 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



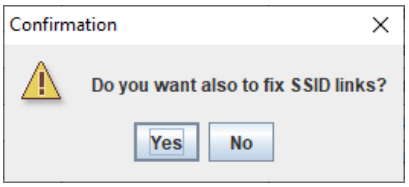

After the button *"Accept"* is clicked, a created SSID will be displayed in *"SSID table"*.

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 *"Create a link"*, the corresponding indicator will turn from yellow to green. Click *"Accept"*.

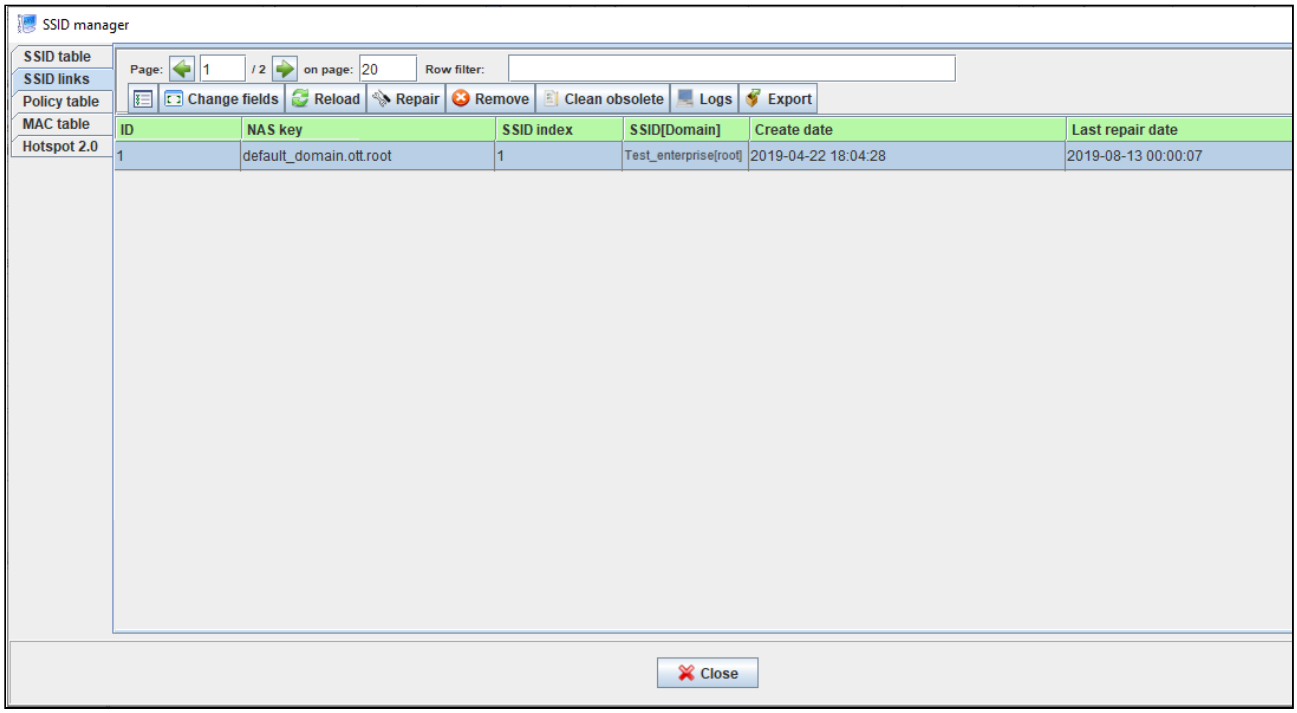



A window with the question "Do you want also to fix SSID links?" will be opened. If it is necessary to assign a created SSID to access points immediately, click "Yes". If a link should be added to the table, but should not be applied to an access point, click "No". If necessary, a SSID can be assigned 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).

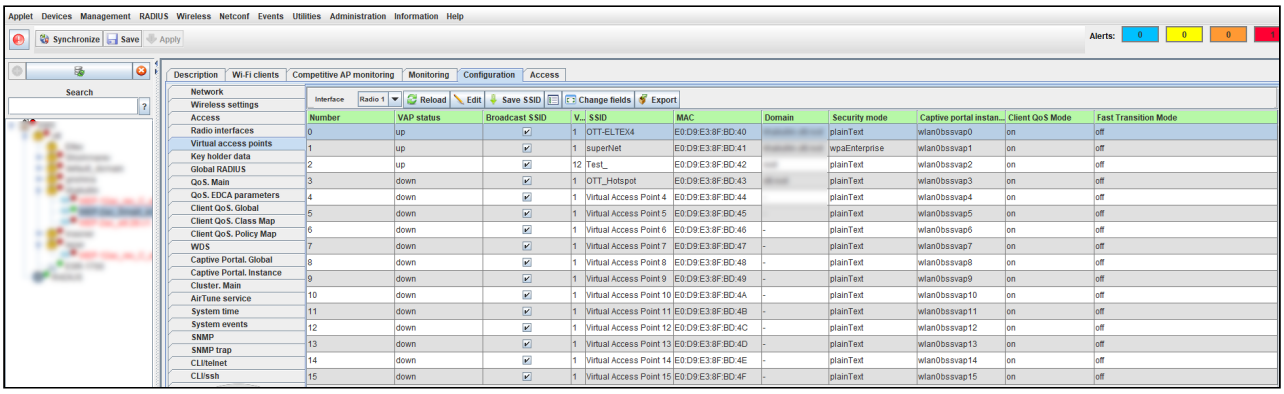



A SSID assigning process can be managed via the tab *"Operations log"*.

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

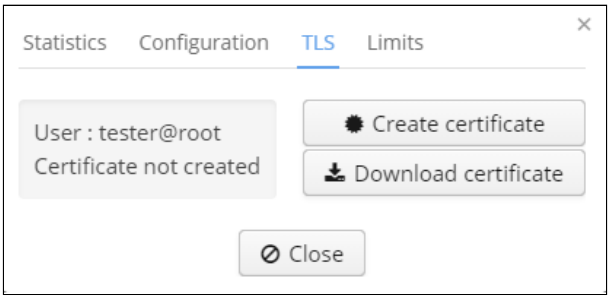


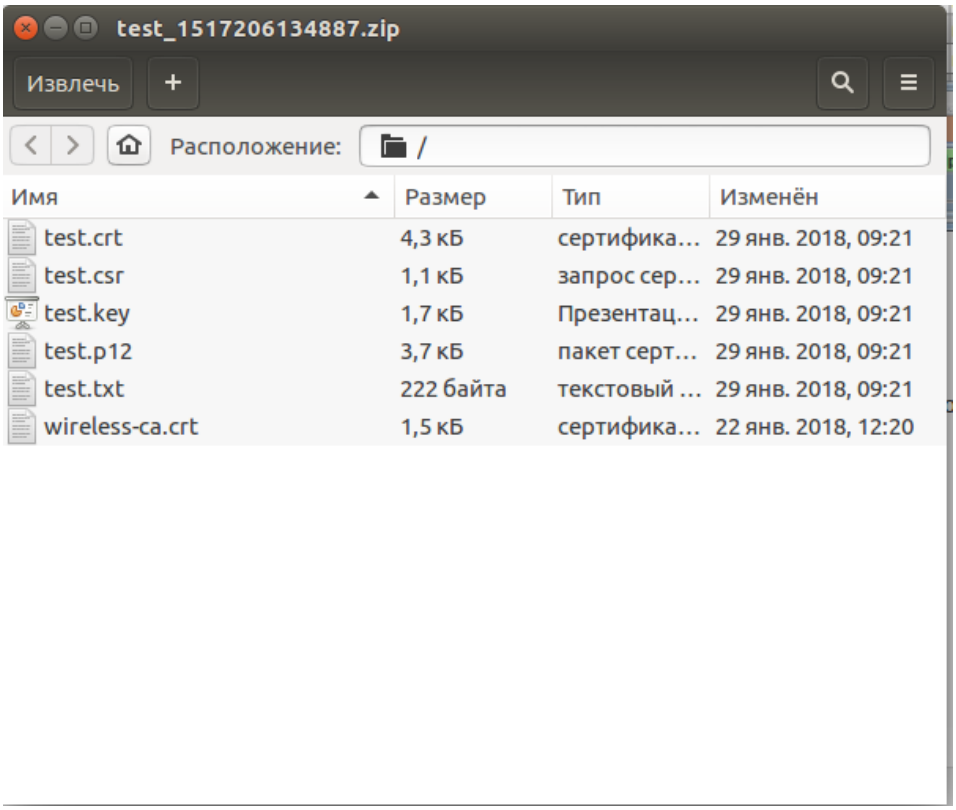

A SSID will be assigned to the first A result can be seen on the tab *"Configuration/Virtual access points"*.




## 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

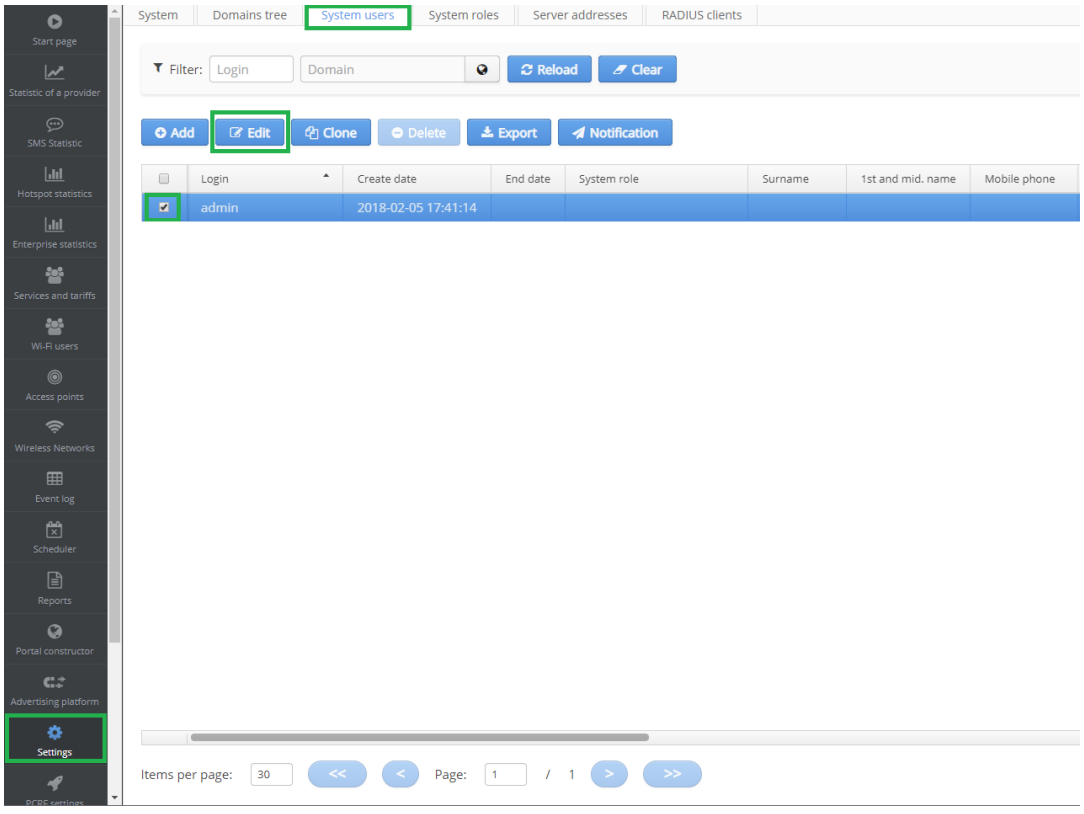
> The value "test" of the "Name" parameter matches the name of the user created via the Admin panel. The value of "Password" is the same.

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

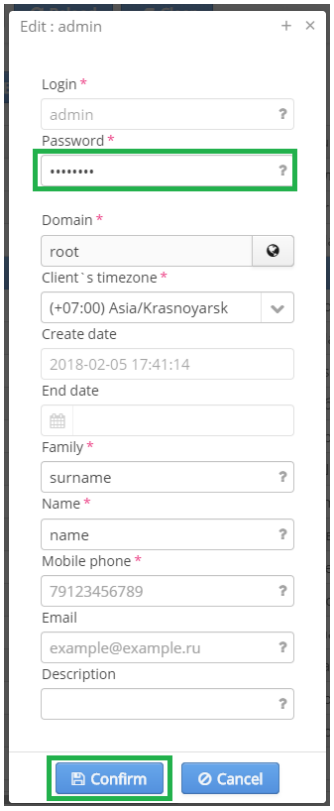
## v1.14_How to change a password for accessing Admin Panel_Portal Constructor (EN)

If packages were installed with default settings, username "admin" and password "password" are used for accessing the Admin Panel and the Portal Constructor.
The password can be changed in the Admin Panel.
To enter the Admin Panel, open your browser and put the server address and the service name into the address bar as follows: http://hostname:8080/wifi-cab/.

To perform authentication, fill in the corresponding fields with the username and the password (admin/password), and then click "*Login*" button or press <Enter>.
Select *"Settings"*, *System users"* tab. Select the check box next to the item with *"admin"* login and click *"Edit"* button.

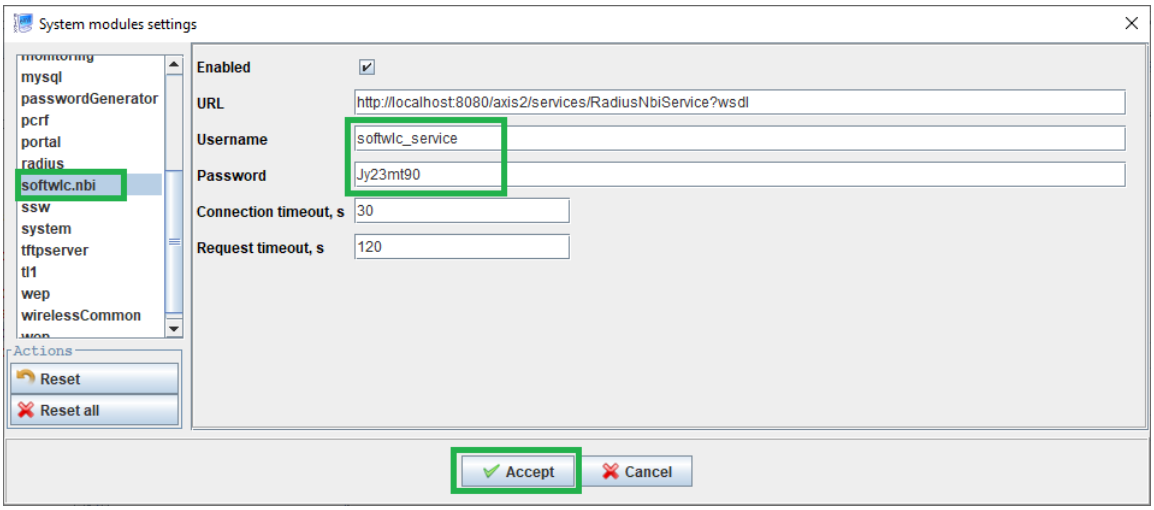



Change the password in the opened window and click *"Confirm"*.

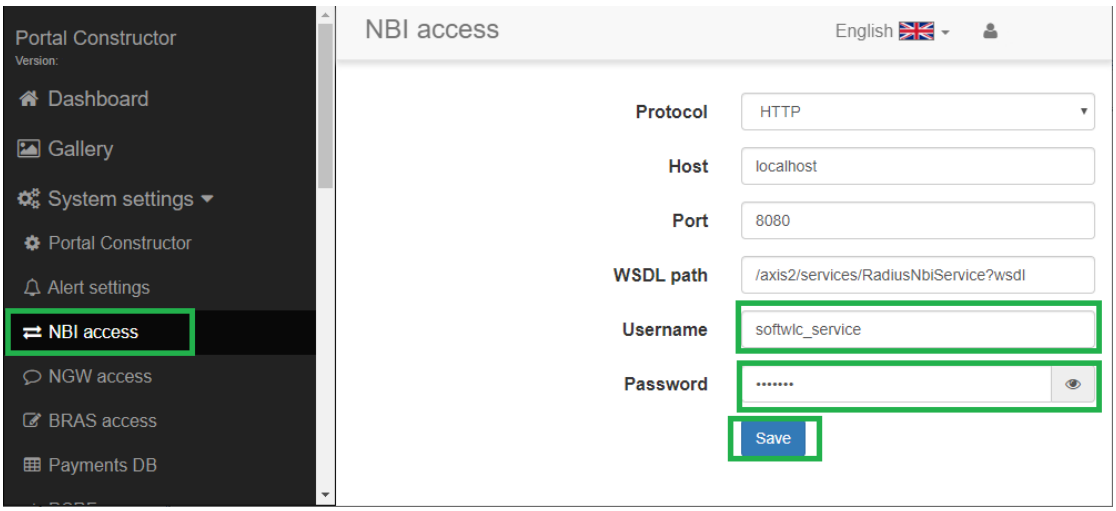



The *admin/password* pair is used in configuration files to provide interaction between system modules. Therefore, once the default password was changed, it must be changed in other sections too.
To avoid getting attached to administrator account, change it to *"softwlc_service"* with *"softwlc"* default password (it can be changed via the Admin Panel as described in this section). This account will be enough for module interaction. However, it has no access to GUI.
The account should be configured/changed in the following sections:

1. **GUI EMS**. Available on http://hostname:8080/ems/jws . Select *"Administration/EMS server configuration/System modules"*. Choose *"softwlc.nbi"*. Specify *"Username"* - *"softwlc_service"*, *"Password"* - *"softwlc"*. Click *"Accept"*.



2. **Portal Constructor.** Available on http://hostname:8080/epadmin . Select *"System settings/NBI access"*. Specify *"Username"* - *"softwlc_service"*, *"Password"* - *"softwlc"*. Click *"Save"*.




3. Configuration file "**/etc/eltex-apb/apb.properties**". Open the file with any available editor, for example *"nano /etc/eltex-apb/apb.properties"* and specify the parameters:

```
nbi.client.login=softwlc_service
nbi.client.password=softwlc
```

To save the changes, press *"Ctrl+o"*, and then <Enter> and *"Ctrl+x"* to quit.

4. Configuration file "**/etc/eltex-wifi-cab/system.xml**". Open the file with any available editor, for example *"nano /etc/eltex-wifi-cab/system.xml"* and specify the parameters:

```
<entry key="nbi.serviceLogin.user">softwlc_service</entry>
<entry key="nbi.serviceLogin.password">softwlc</entry>
```

To save the changes, press *"Ctrl+o"*, then <Enter> and *"Ctrl+x"* to quit.

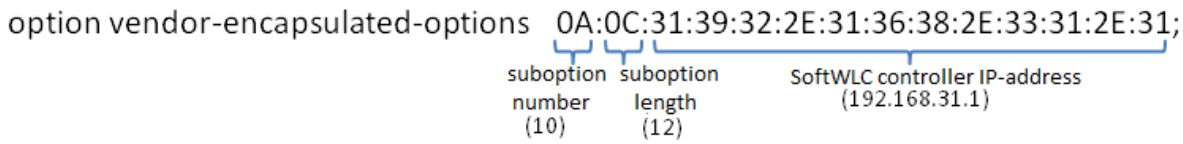
After changing the passwords, restart EMS and tomcat7:

```
sudo service eltex-ems restart
sudo service tomcat7 restart
```

v1.14_How to configure option 43, and other DHCP configuration aspects (EN)

## Configuring option 43 for automatic connection to SoftWLC (10 suboption)

It is necessary to configure suboption 10 (option 43) containing SoftWLC IP address on DHCP server for an access point to send an SNMP trap to SoftWLC when connected to the network. IP address is presented in hexadecimal format.
Example:




The option is formed in the following way:

**0A –** suboption number. This code represents the number 10 because suboption 10 is used for SoftWLC IP address transmitting;

**0C** – SoftWLC IP address length. It will change depending on the address.

For example, SoftWLC IP address is 192.168.31.1. It consists of 12 symbols.


Consequently, the address' length is represented by 0C in hexadecimal format; ;

**31:39:32:2E:31:36:38:2E:33:31:2E:31** – SoftWLC IP address encoded in ASCII (HEX), where:

31 - 1

39 - 9

32 - 2

2E - decimal point

31 - 1

36 - 6

38 - 8

2E - decimal point

33 - 3

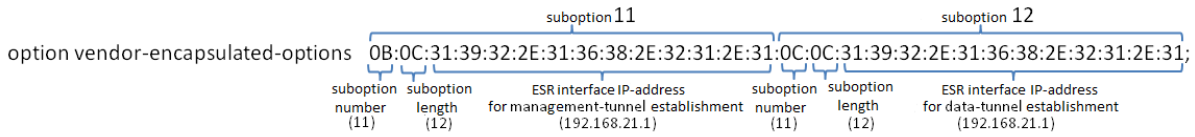
31 - 1

2E - decimal point

31 - 1

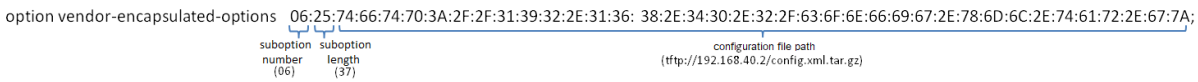
## Configuring option 43 for creating GRE tunnels between access points and ESR-1000 (suboptions 11 and 12)

To create GRE tunnels, configure suboption 11 containing ESR IP address for management-tunnel and suboption 12 containing ESR IP address for data-tunnel in option 43. IP address is presented in hexadecimal format.
Example:



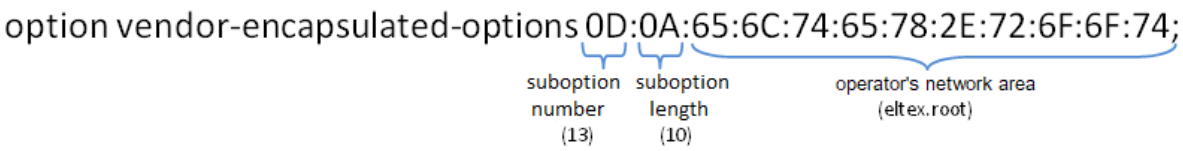

## Configuring option 43 for AP autoconfiguration (suboption 6)

To provide AP autoconfiguration, configure suboption 6 containing congifuration file path in hexadecimal format in option 43.
Example:



## Configuring option 43 for identifying carrier network area the access point belongs to (suboption13)

To indicate that an access point belongs to a specific carrier network area, configure suboption 13 (in hexadecimal format) containing the name of the area in option 43.
Example:




## Configuring the class for IP address allocation depending on Relay Agent IP address

To provide IP address allocation depending on Relay Agent IP address, configure the class containing DHCP relay IP address. For example, (binary-to-ascii(10,8, ".", packet(24,4)) = "120.10.10.10"). Since then, the class should be specified in DHCP address pool.

## Configuring the class for IP address allocation depending on Vendor Class Identifier

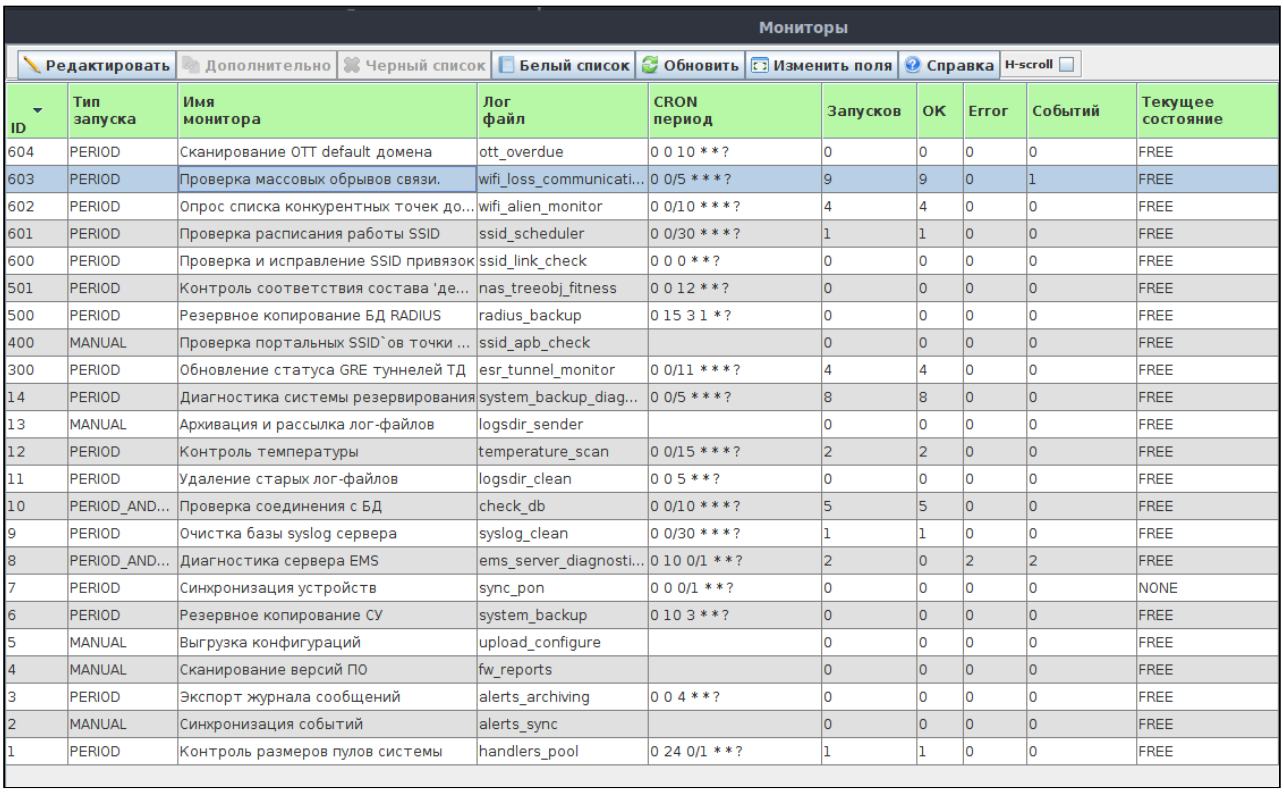
To provide IP address allocation depending on Vendor Class Identifier, the class containing the code of option 60 (sent by an access point in request) should be configured. For example, (substring (optionvendor-class-identifier, 0, 14) = "ELTEX_WEP-12AC"). Since then, the class should be specified in DHCP address pool.

**DHCP server configuration example:**

```
class "wep_tunnel_ip" {
    match if (
    ((binary-to-ascii(10,8, ".", packet(24,4)) = "10.0.10.1") # DHCP relay IP address 10.0.10.1
        and
    ((substring (option vendor-class-identifier, 0, 14) = "ELTEX_WEP-12AC") or (substring (option
vendor-class-identifier, 0, 14) = "ELTEX_WOP-12AC"))
                );
                                }

class "data" {
    match if ((binary-to-ascii(10,8, ".", packet(24,4)) = "10.0.12.1") # DHCP relay IP address
10.0.12.1);
                  }

class "mgmt" {
    match if (
        ((binary-to-ascii(10,8, ".", packet(24,4)) = "10.0.11.1") # DHCP relay IP address 10.0.
11.1)
        and
        ((substring (option vendor-class-identifier, 0, 14) = "ELTEX_WEP-12AC") or (substring
(option vendor-class-identifier, 0, 14) = "ELTEX_WOP-12AC"))
                 );
                   }

shared-network WEP {
    subnet 10.0.1.0 netmask 255.255.255.0 {}
    subnet 10.0.10.0 netmask 255.255.255.0 {}
    subnet 10.0.11.0 netmask 255.255.255.0 {}
    subnet 10.0.12.0 netmask 255.255.255.0 {}

pool {
    option routers 10.0.10.1;
    option vendor-encapsulated-options 0B:09:31:30:2E:30:2E:31:31:2E:31:0C:09:31:30:2E:30:2E:31:
32:2E:31;
    # ESR interface IP address, 10.0.11.1 for management-tunnel, 10.0.12.1 for data-tunnel
    range 10.0.10.20 10.0.10.25;
    allow members of "wep_tunnel_ip";
        }

pool {
    option routers 10.0.11.1;
    option vendor-encapsulated-options 0A:08:31:30:2E:30:2E:31:2E:31;  # SoftWLC IP address 10.0.
1.1
    range 10.0.11.20 10.0.11.25;
    allow members of "mgmt";
        }

pool {
    option routers 10.0.12.1;
    range 10.0.12.20 10.0.12.25;
```

```
    allow members of "data";
        }
}
```

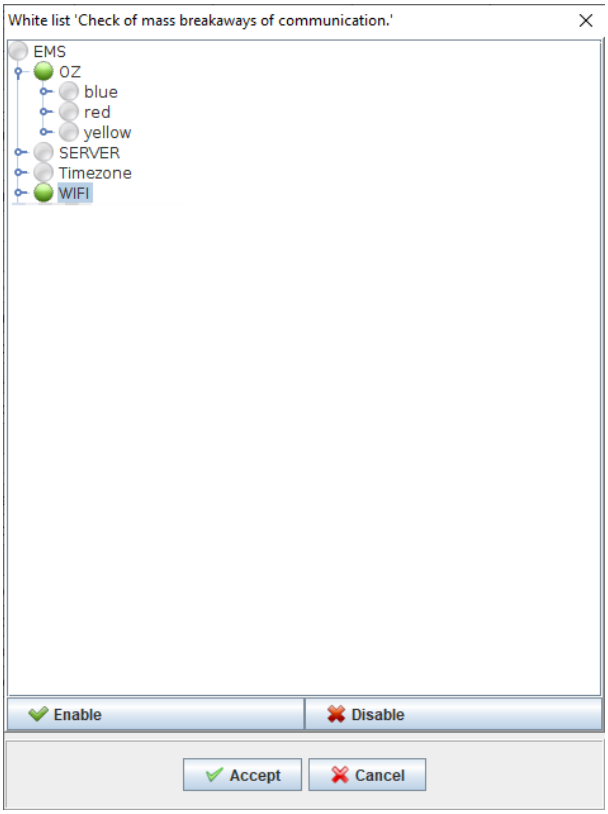
## v1.14_Setting up AP group monitoring on a node (EN)



Мониторы

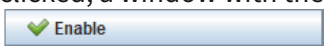
Редактировать | Дополнительно | Черный список | Белый список | Обновить | Изменить поля | Справка | H-scroll

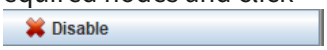
| ID | Тип запуска | Имя монитора | Лог файл | CRON период | Запусков | OK | Error | Событий | Текущее состояние |
|---|---|---|---|---|---|---|---|---|---|
| 604 | PERIOD | Сканирование OTT default домена | ott_overdue | 0 0 10 * * ? | 0 | 0 | 0 | 0 | FREE |
| 603 | PERIOD | Проверка массовых обрывов связи. | wifi_loss_communicati... | 0 0/5 * * * ? | 9 | 9 | 0 | 1 | FREE |
| 602 | PERIOD | Опрос списка конкурентных точек до... | wifi_alien_monitor | 0 0/10 * * * ? | 4 | 4 | 0 | 0 | FREE |
| 601 | PERIOD | Проверка расписания работы SSID | ssid_scheduler | 0 0/30 * * * ? | 1 | 1 | 0 | 0 | FREE |
| 600 | PERIOD | Проверка и исправление SSID привязок | ssid_link_check | 0 0 0 * * ? | 0 | 0 | 0 | 0 | FREE |
| 501 | PERIOD | Контроль соответствия состава 'де... | nas_treeobj_fitness | 0 0 12 * * ? | 0 | 0 | 0 | 0 | FREE |
| 500 | PERIOD | Резервное копирование БД RADIUS | radius_backup | 0 15 3 1 * ? | 0 | 0 | 0 | 0 | FREE |
| 400 | MANUAL | Проверка портальных SSID`ов точки ... | ssid_apb_check | | 0 | 0 | 0 | 0 | FREE |
| 300 | PERIOD | Обновление статуса GRE туннелей ТД | esr_tunnel_monitor | 0 0/11 * * * ? | 4 | 4 | 0 | 0 | FREE |
| 14 | PERIOD | Диагностика системы резервирования | system_backup_diag... | 0 0/5 * * * ? | 8 | 8 | 0 | 0 | FREE |
| 13 | MANUAL | Архивация и рассылка лог-файлов | logsdir_sender | | 0 | 0 | 0 | 0 | FREE |
| 12 | PERIOD | Контроль температуры | temperature_scan | 0 0/15 * * * ? | 2 | 2 | 0 | 0 | FREE |
| 11 | PERIOD | Удаление старых лог-файлов | logsdir_clean | 0 0 5 * * ? | 0 | 0 | 0 | 0 | FREE |
| 10 | PERIOD_AND... | Проверка соединения с БД | check_db | 0 0/10 * * * ? | 5 | 5 | 0 | 0 | FREE |
| 9 | PERIOD | Очистка базы syslog сервера | syslog_clean | 0 0/30 * * * ? | 1 | 1 | 0 | 0 | FREE |
| 8 | PERIOD_AND... | Диагностика сервера EMS | ems_server_diagnosti... | 0 10 0/1 * * ? | 2 | 0 | 2 | 2 | FREE |
| 7 | PERIOD | Синхронизация устройств | sync_pon | 0 0 0/1 * * ? | 0 | 0 | 0 | 0 | NONE |
| 6 | PERIOD | Резервное копирование СУ | system_backup | 0 10 3 * * ? | 0 | 0 | 0 | 0 | FREE |
| 5 | MANUAL | Выгрузка конфигураций | upload_configure | | 0 | 0 | 0 | 0 | FREE |
| 4 | MANUAL | Сканирование версий ПО | fw_reports | | 0 | 0 | 0 | 0 | FREE |
| 3 | PERIOD | Экспорт журнала сообщений | alerts_archiving | 0 0 4 * * ? | 0 | 0 | 0 | 0 | FREE |
| 2 | MANUAL | Синхронизация событий | alerts_sync | | 0 | 0 | 0 | 0 | FREE |
| 1 | PERIOD | Контроль размеров пулов системы | handlers_pool | 0 24 0/1 * * ? | 1 | 1 | 0 | 0 | FREE |




Node monitoring and sending integral alerts by e-mail are carried out by EMS "Check of mass breakaways of communication" monitor. The monitor supervises a certain node or a group of nodes. If a node includes nested nodes, the monitors will consider them too.
Configurable parameters of the monitor:
Period which is set to 10 minutes by defaultPercent — percent of devices with communication breakaway above which an alert is generated (50 percent by default)

To set up the monitor, a node should be added to a whitelist 

. When "Whitelist" button is clicked, a window with the list of nodes opens. Select required nodes and click 

to add a node to the list or 

to delete it. After the selection, the node turns green. Click "Accept" button.
The monitor is set up, from now on, an integral alert will be sent to a predetermined e-mail of EMS user in case of communication failure (on more than 50% of the devices by default).

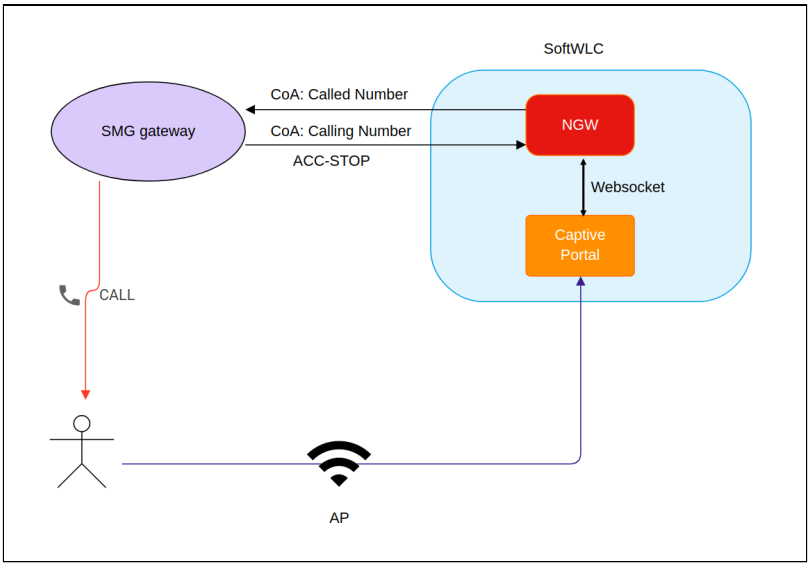
⚠ To get notifications by e-mail, "Sending alert messages to e-mail" should be set.

## v1.14_Configuring call back authorization (EN)


- Interaction scheme
  - Description

- Configuring call back authorization
    - Troubleshooting
- Identification scenario
- SMG configuration


## 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

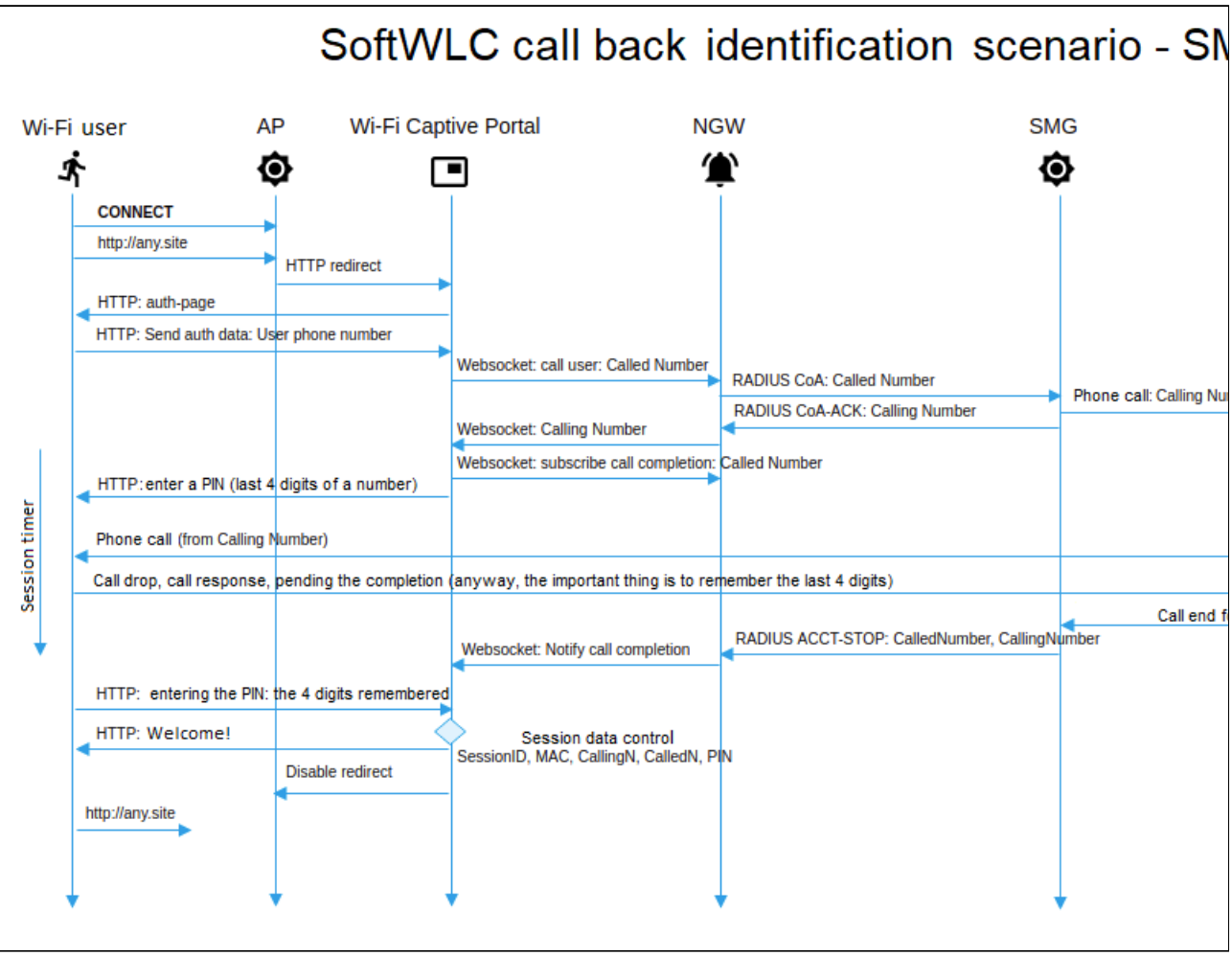
-Make sure that the keys specified for eltex-ngw and for SMG gateway are equal by checking them in the section "RADIUS Authorization servers". If the keys do not match, the gateway will not respond the CoA requests from eltex-ngw.

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
```

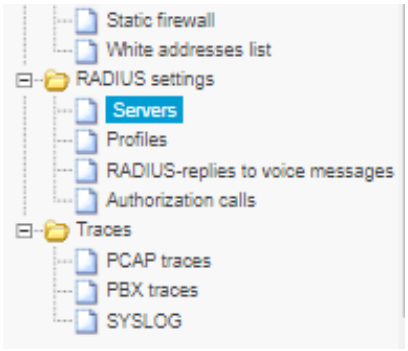
If a number specified by a user cannot be called, SMG will respond with a CoA-NAK message without any attributes and will not initiate a call. If a CoA Request was sent from a RADIUS server that is not linked to the selected RADIUS profile, or it was sent to a network interface that does not correspond 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:

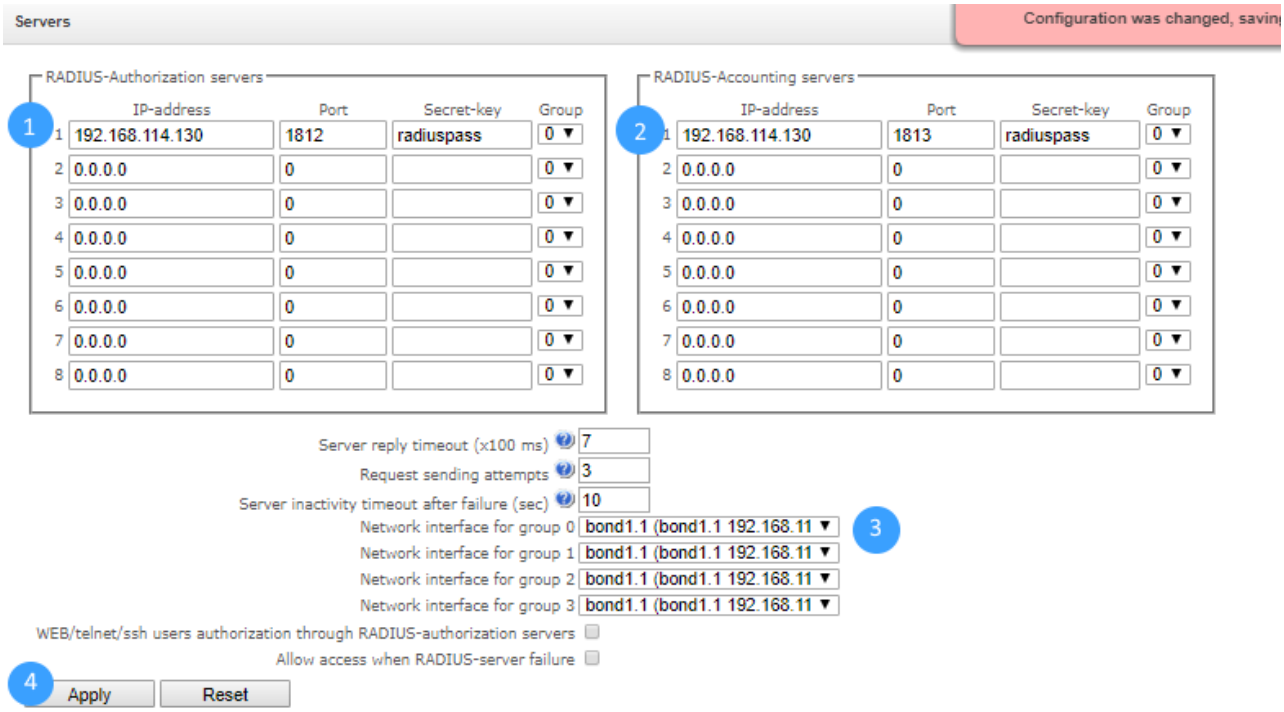
- PBX profile – PBX profile link;
- RADIUS profile – a profile that will be used to send Accounting requests. RADIUS CoA requests from servers linked to this profile can be accepted;
- Dial plan – dial plan link for call routing;
- Access category – access category selecting;

- 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.

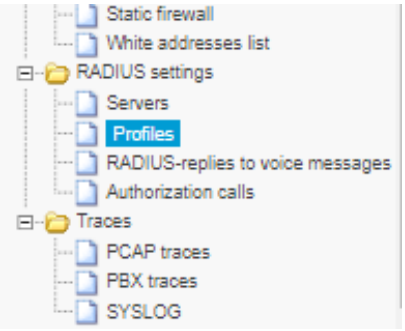
**To configure the service:**
Open the section "RADIUS settings -> Servers"



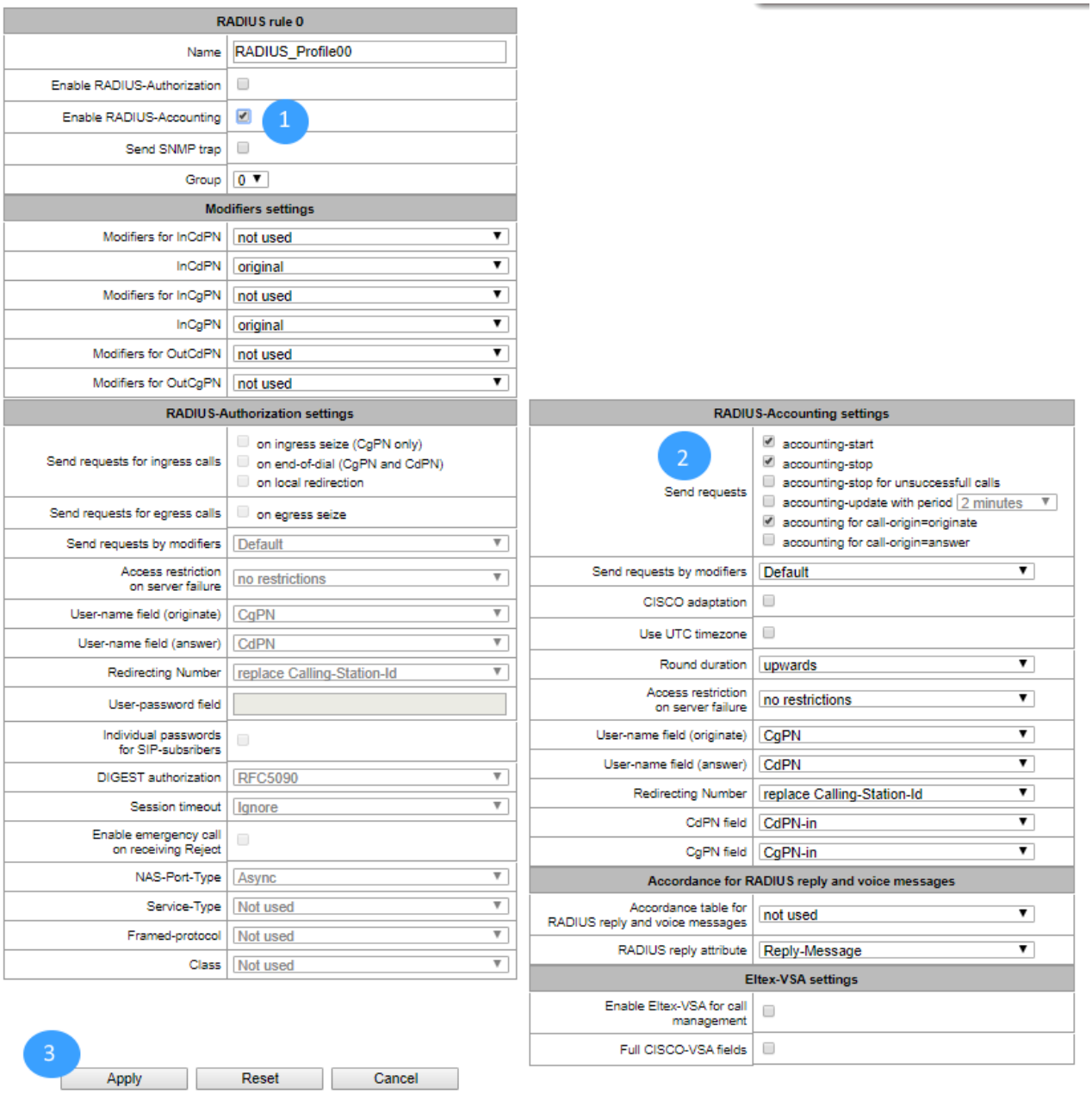

1 - Specify an address of a server from which a RADIUS CoA request will be sent;
1 - Specify an address of a server to which RADIUS Accounting will be sent;
3 - Choose a network interface that will be used for interaction;
4 - Apply the changes.



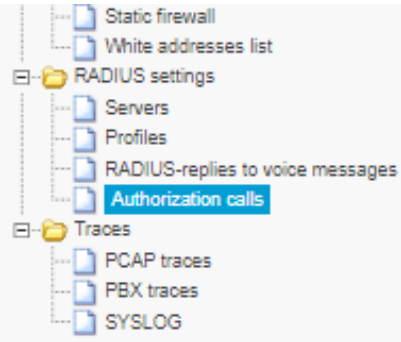

Open the section "RADIUS settings -> Profiles"




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

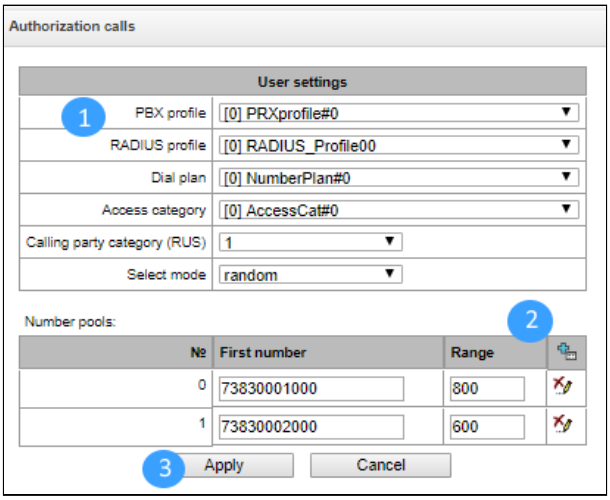



Open the section "RADIUS settings -> Authorization calls"




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.




## v1.14_Configuring trap sending via Syslog protocol (EN)

1. Edit the following lines of the /usr/lib/eltex-ems/conf/log4j.xml configuration file:

- Configure IP address of a Syslog server<Syslog name="TrapSyslog" format="RFC5424" host="**192.168.1.1**" port="514"
- Set INFO logging level<ThresholdFilter level="**INFO**" onMatch="ACCEPT" onMismatch="DENY"/>
- Set INFO logging level for the logger under TRAP_SYSLOG name (set to OFF by default)

```
<logger name="TRAP_SYSLOG" level="INFO" additivity="false">
      <appender-ref ref="TrapSyslog"/>
 </logger>
```

2. Set **INFO** logging level on Syslog server.

# v1.14_Setting tariffs for portal authorization (EN)

## Creating a tariff with captive portal authorization

To create a new tariff, select the "Tariff management" tab of the "RADIUS" menu and click the button "Add". Fill in the following fields in the opened window:

- Tariff name;
- Tariff code;
- Domain;
- Tariff description;
- Set "Deactivated" checkbox to enable portal authorization.

When "Deactivated" checkbox is checked, the following parameters for portal authorization scripts become available for editing:

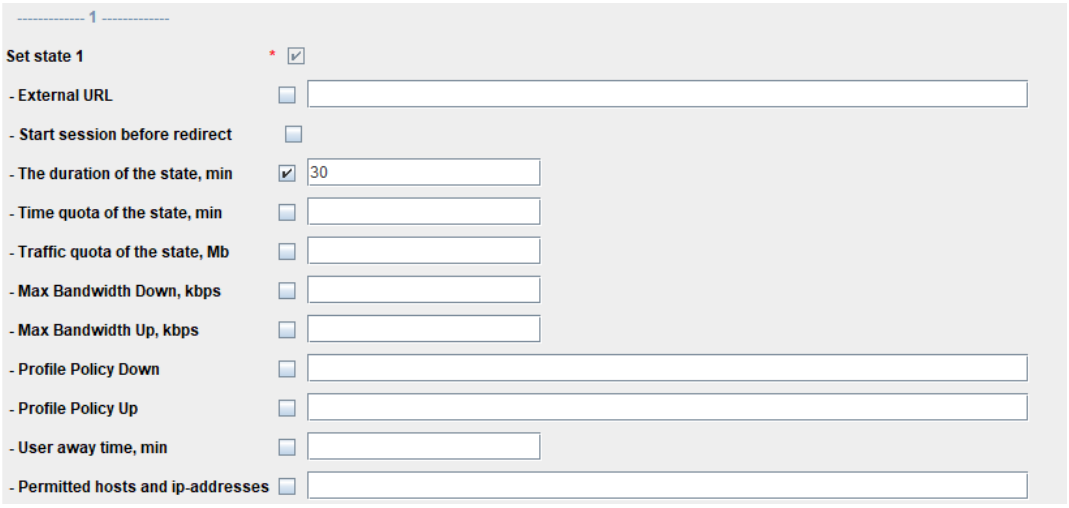
- Set state N — enable state N (the first one is always enabled by default);
- External URL — URL address for user redirection after registration is completed;
- Start session before redirect — when the checkbox is set, a session starts before redirection to an external URL address;
- The duration of the state, min — maximum duration of state N in minutes;
- Time quota of the state — common quota for all user sessions within state N in minutes;
- Traffic quota of the state — common quota for user downstream traffic within state N in megabytes;
- Max Bandwidth Down/Up, kbps — bandwidth limit for user downstream and upstream traffic within state N in kbps;
- Profile Policy Down/Up — Policy profile for a specific downstream user within state N;
- User away time, min — time during which user authorization information for state N is keeped on AP (in minutes);
- Permitted hosts and IP addresses — the list of DNS and IP addresses that are accessible to the user. To enable functionality, the external URL address should be configured. Permitted addresses should be separated by a comma.
- Period for switching to next state — a cron expression at which the switch to next state happens. To enable the functionality, cron period should be specified.

## Script examples

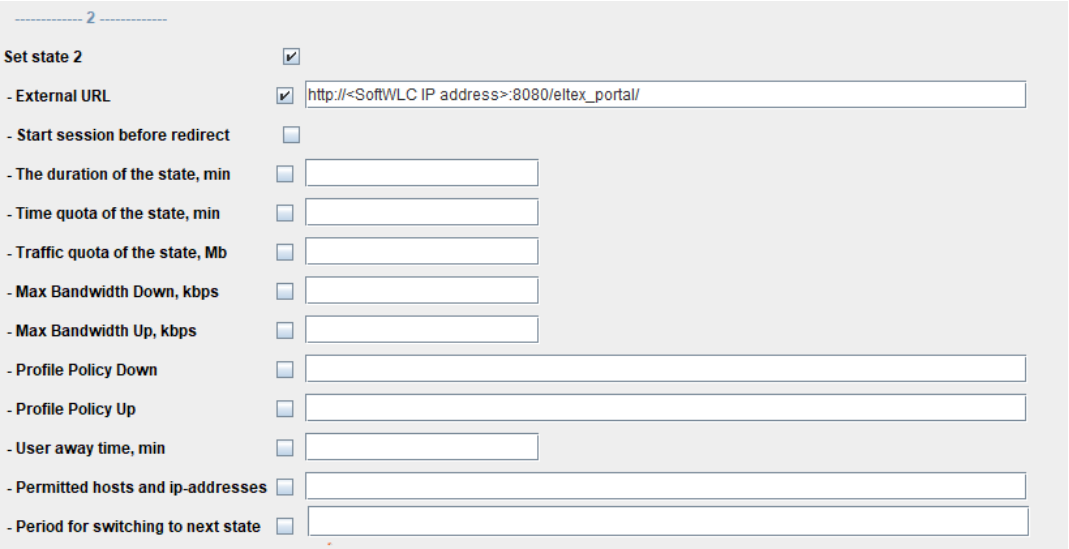
Several examples of typical states used for portal authorization will be considered below.

## Tariff with time limit

***Description:*** within the tariff a user with portal authorization is granted time-limited Internet access. When the limit is exceeded, a user will be redirected to the session timeout page and informed of the session termination reason. After clicking the close button, a user will be redirected to the authorization page.
***Configuration:*** to set the tariff with time limit, enable "The duration of state" parameter in state 1 and define time limit in minutes.



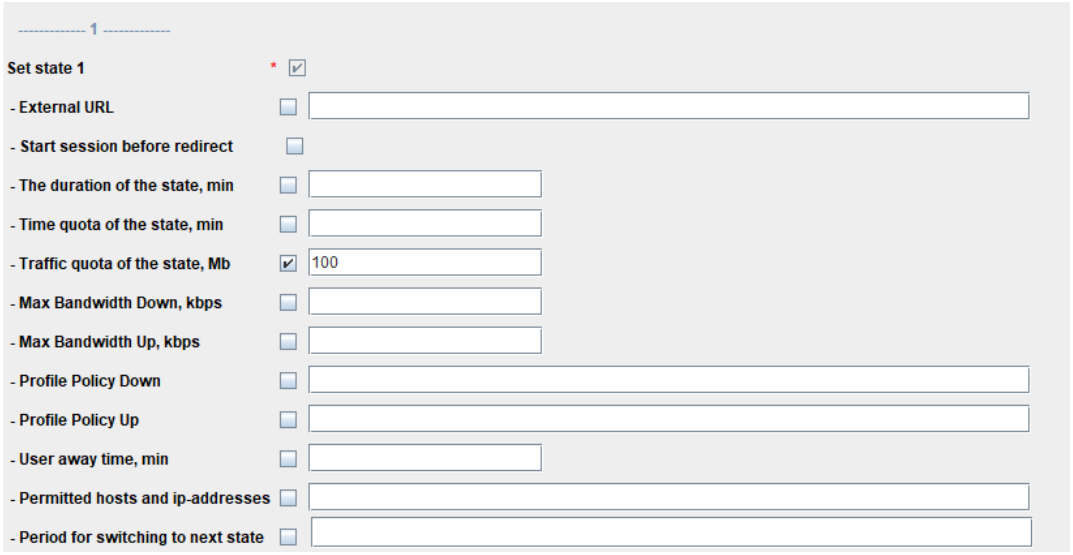

For the session timeout page to be displayed on expiry of time limit, enable state 2 and provide a link to captive portal in "External URL" field.



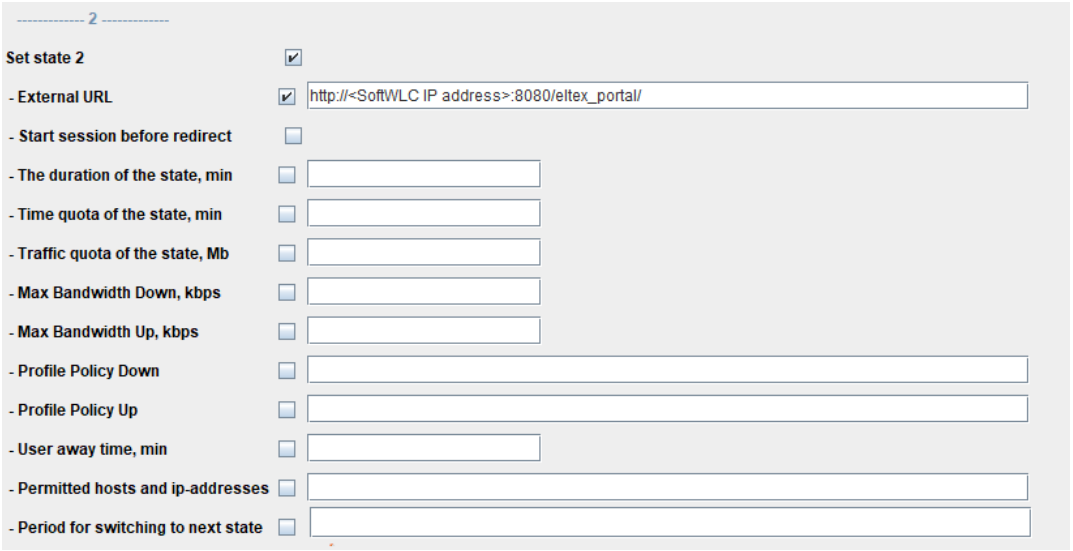

## Tariff with traffic quota

***Description:*** within the tariff a user with portal authorization is granted Internet access with traffic quota. When the limit is exceeded, a user will be redirected to the session timeout page and informed of the session termination reason. After clicking the close button, a user will be redirected to the authorization

page.
***Configuration:*** to set the tariff with tariff quota, enable "Traffic quota of the state" parameter in state 1 and define traffic quota in Mb.



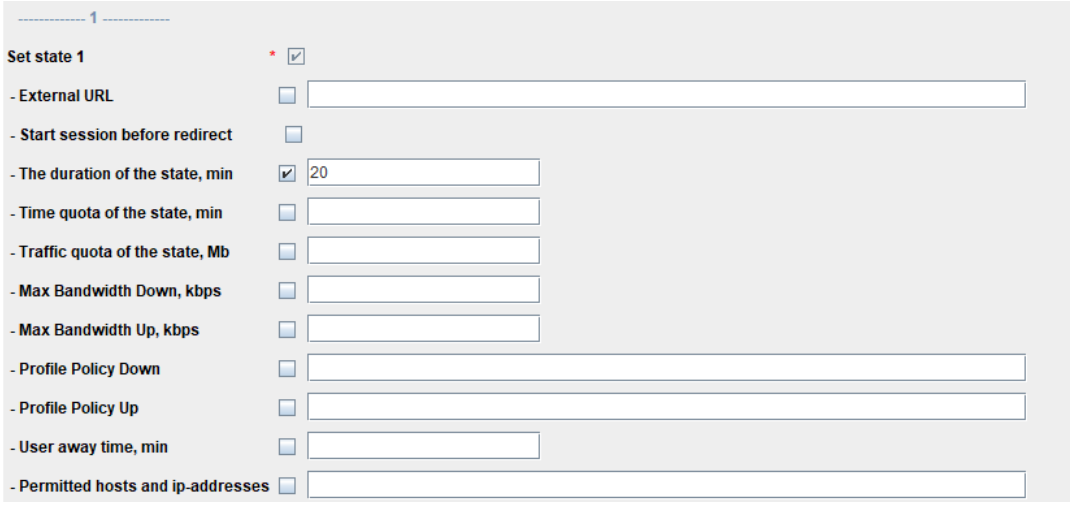

For the session timeout page to be displayed on expiry of time limit, enable state 2 and provide a link to captive portal in "External URL" field.



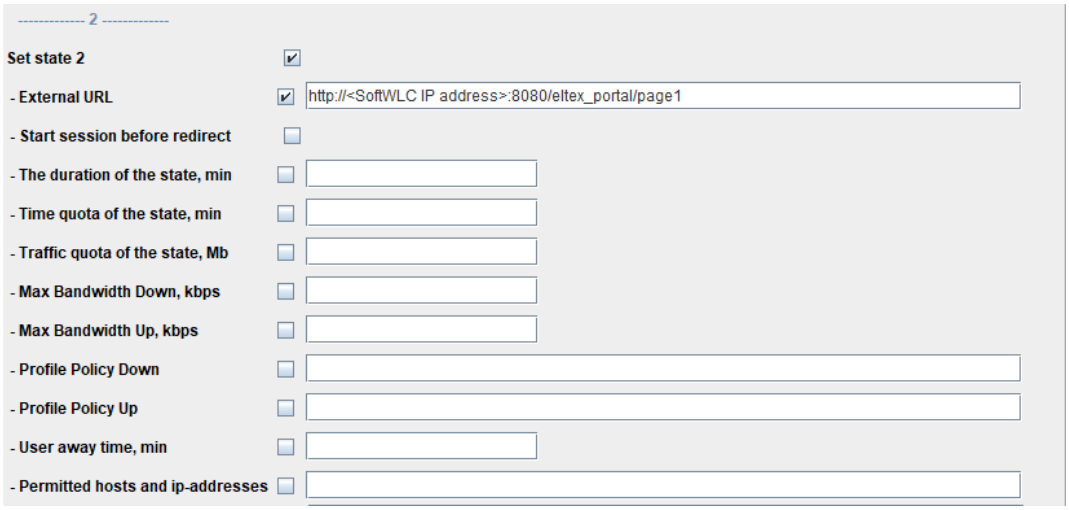

## Tariff with bandwidth limit that changes at certain intervals

***Description:*** the tariff consists of 3 cases:
1. The duration of the state is 20 minutes, no bandwidth limit. After this state, a user is redirected to a page created in portal settings.
2. The duration of the state is 30 minutes, max Bandwidth Down/Up is 10 Mbps. The state is entered after clicking "Continue" button on the state 1 page.
3. The duration of the state is 30 minutes, max Bandwidth Down/Up is 2 Mbps. After this state, a user is redirected to the session timeout page.

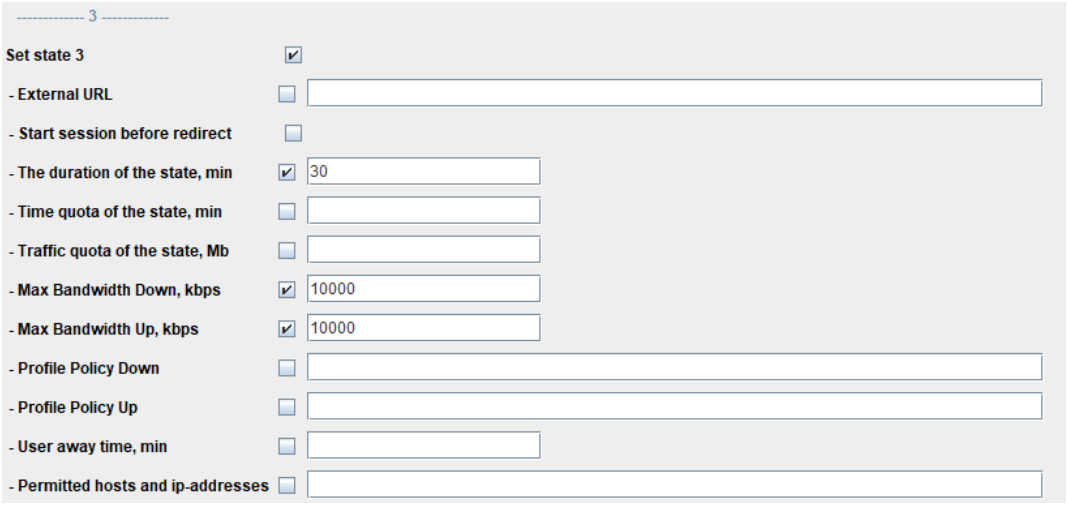
***Configuration:*** to configure the first case, enable "The duration of the state" field in state 1 and define 20-minute time limit.




To set redirection to the page created in portal settings, enable state 2 and provide a link to http://<ip">http://<SoftWLC ip address>:8080/eltex_portal/page1 in "External URL address".




To configure the second case, enable "The duration of the state" field in state 3 and define 30-minute time limit. To set bandwidth limit, enable "Max Bandwidth Down" and "Max Bandwidth Up" fields and define 10 000 kbps limit.

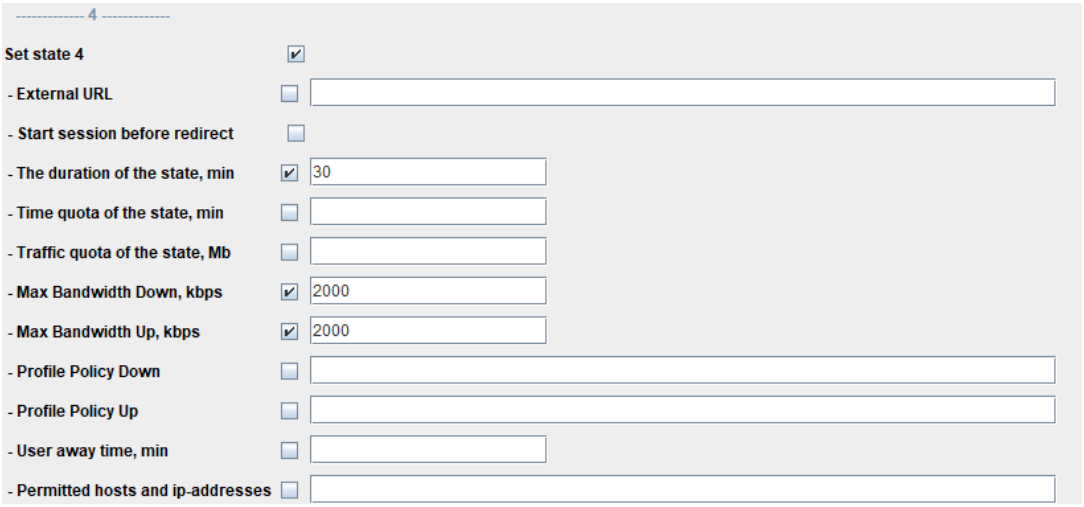



To configure the third case, enable "The duration of the state" field in state 4 and define 30-minute time limit. To set bandwidth limit, enable "Max Bandwidth Down" and "Max Bandwidth Up" fields and define 2 000 kbps limit.

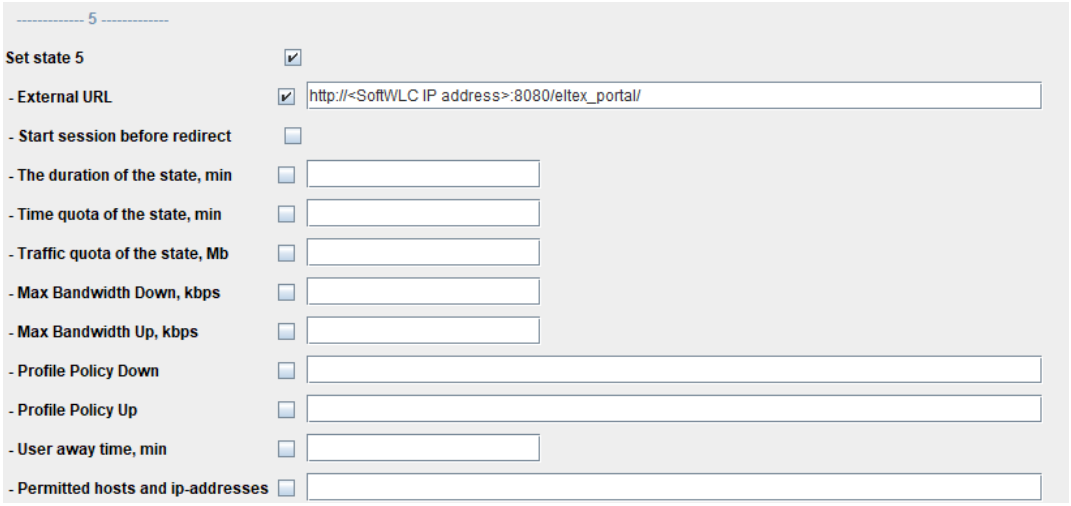
***Description:*** the tariff consists of 3 cases:

1. The duration of the state is 20 minutes, no bandwidth limit. After this state, a user is redirected to a page created in portal settings.
2. The duration of the state is 30 minutes, max Bandwidth Down/Up is 10 Mbps. The state is entered after clicking "Continue" button on the state 1 page.
3. The duration of the state is 30 minutes, max Bandwidth Down/Up is 2 Mbps. After this state, a user is redirected to the session timeout page.

***Configuration:*** to configure the first case, enable "The duration of the state" field in state 1 and define 20-minute time limit.

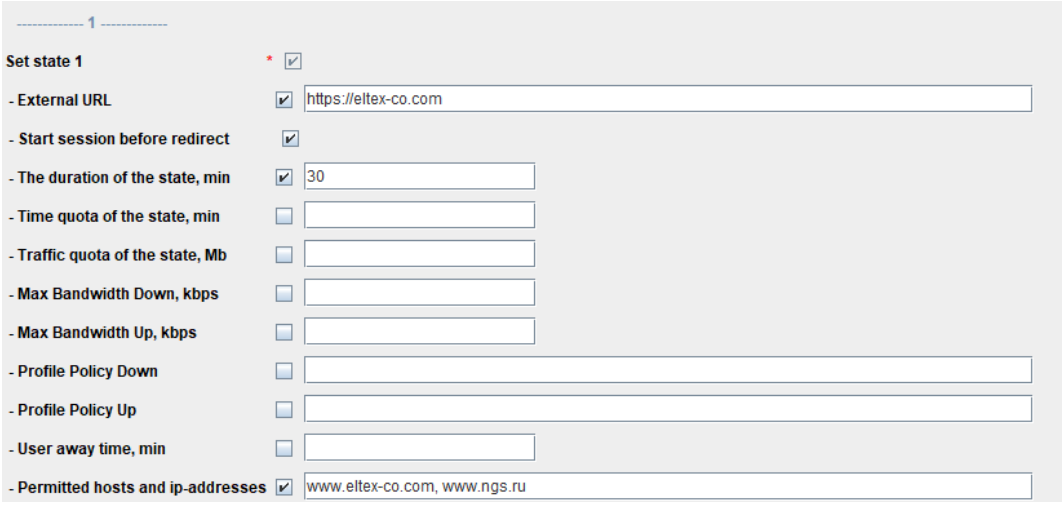



For the session termination page to be displayed, enable state 5 after the third case is completed and provide a link to captive portal.

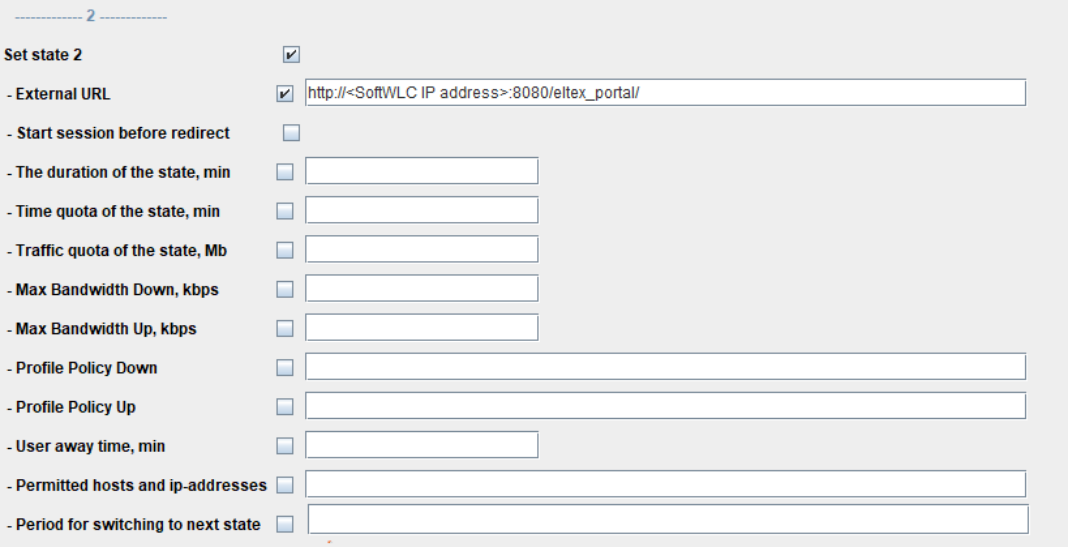



## Tariff with limited access to resources

***Description:*** within this tariff, a user is granted access to certain resources. When a user tries to open a resource that is not permitted, redirection to an external URL address is done. "The duration of the state" and "Start session before redirect" should be also set.
***Configuration:*** to configure the tariff with limited access to resources, enable "External URL" parameter and provide URL address for user redirection after registration. Specify dns and ip addresses in "Permitted hosts and ip-addresses" field. Enable "Start session before redirect" and "The duration of the state ". Define time limit in minutes.




For the session timeout page to be displayed on expiry of time limit, enable state 2 and provide a link to captive portal in "External URL" field.

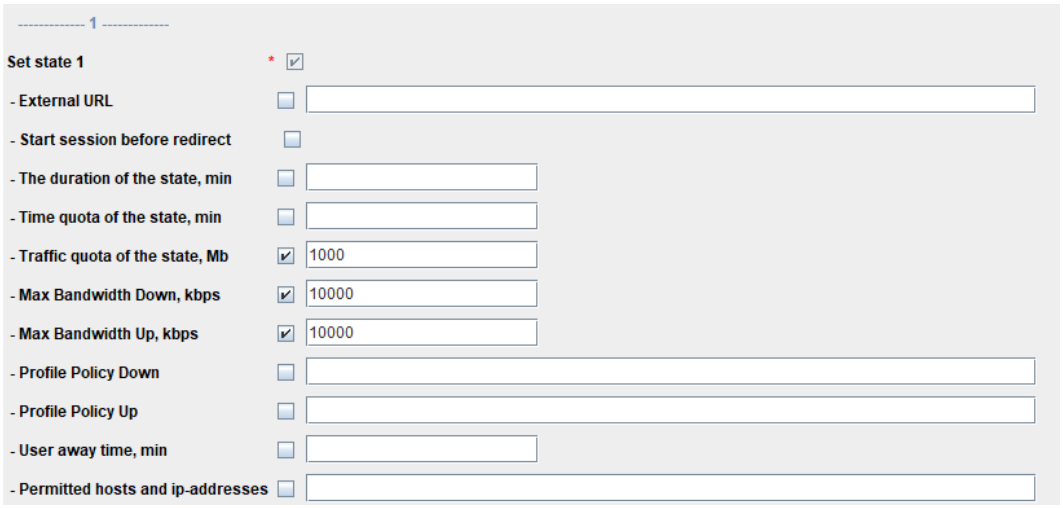



***Note!*** For the tariff to work correctly on an access point, DNS server access should be configured on it

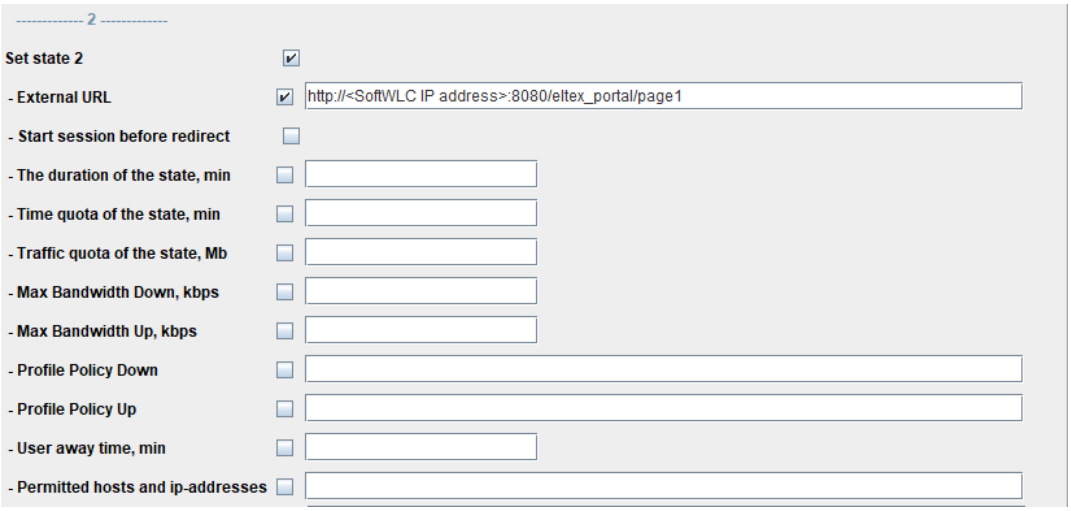
### Tariff with periodic bandwidth limit change

***Description:*** The tariff consists of 2 cases:
1. The duration of the state is not limited, Traffic quota of the state is 1 Gb, and Bandwidth limit is 10 Mbps. After the case is completed, a user is redirected to the page created in portal settings with notification on the quota.
2. The duration of the state is 10000 minutes, max Bandwidth Down/Up is 1 Mbps and Period for switching to next state is once a day at 0:00. The state is entered after clicking "Continue" button on the state 1 page.

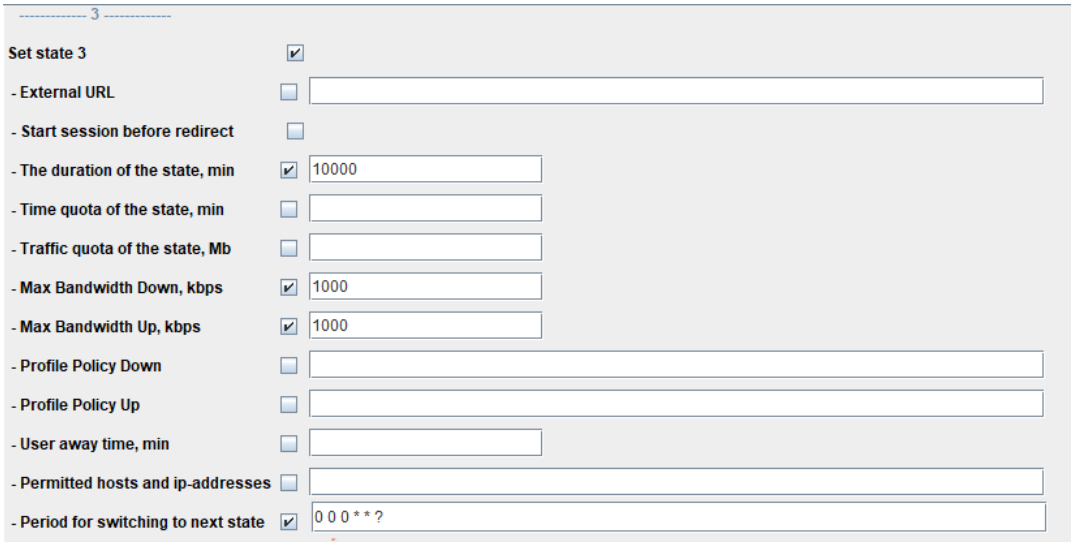
***Configuration:*** to configure the first case, enable "Traffic quota of the state" field in state 1 and define 1000 Mb traffic quota. To set bandwidth limit, enable "Max Bandwidth Down" and "Max Bandwidth Up" fields and define 10 000 kbps limit.




To set redirection to the page created in portal settings, enable state 2 and provide a link to the page created in Portal Constructor http://<ip">http://<SoftWLC ip address>:8080/eltex_portal/page1 in "External URL address"




To configure the second case, enable state 3 and define 1000 kbps limit in "Max Bandwidth Down" and "Max Bandwidth Down" fields. Set "Period for switching to the next state" to "once a day at 0:00" and define "The duration of the state" that should be higher than the first parameter.

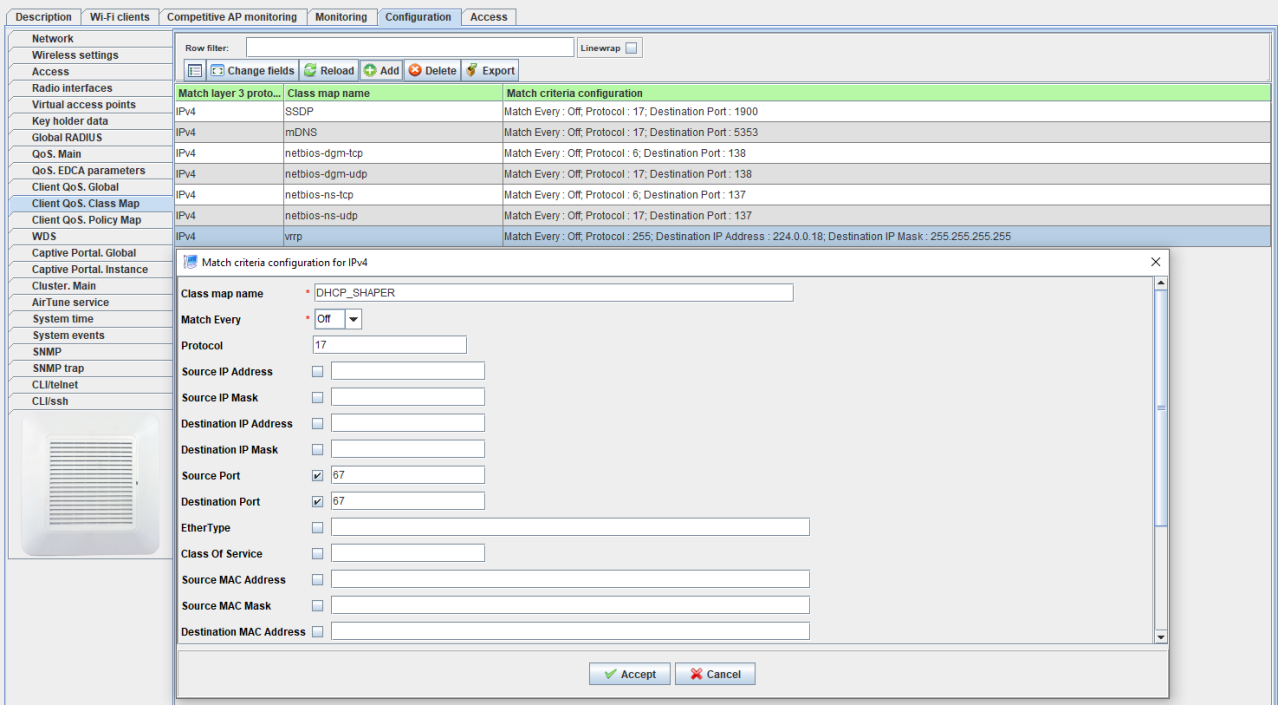



After 0:00, a user will switch to next state (to the first state for the example considered, as there are no more states enabled).

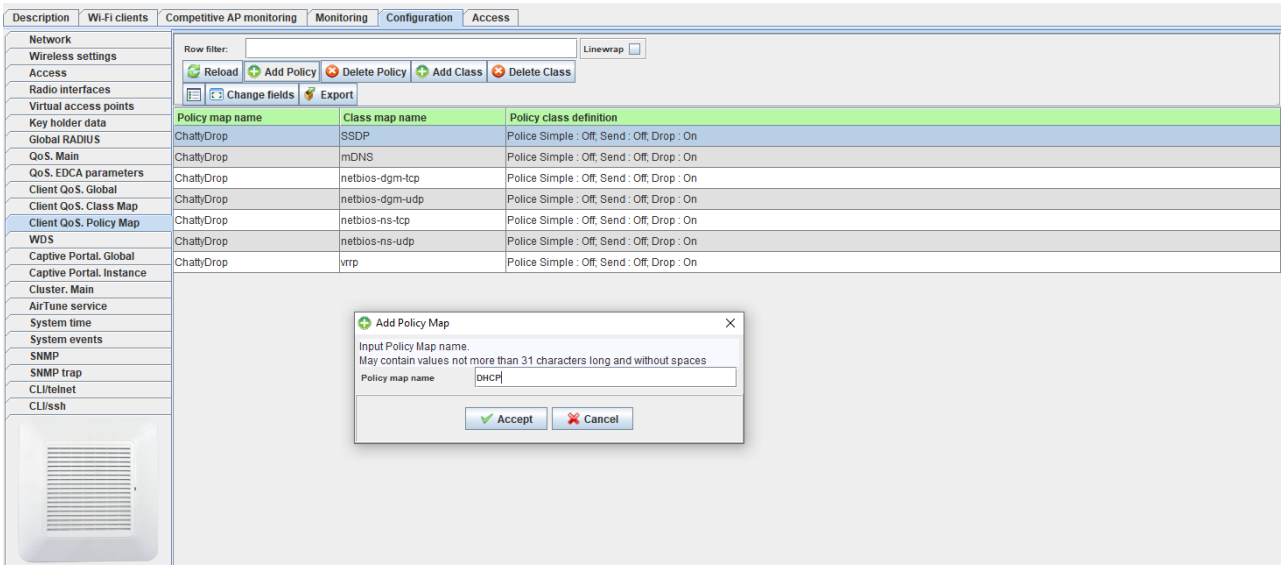
## v1.14_Setting 'Rate limit' (DHCP traffic) on AP and ESR (EN)

To configure DHCP shaper via EMS on an access point:

1. Select Configuration
2. Select Client.QoS Class Map tab
3. Add a required class
4. Protocol = 17 (UDP), Source/Destination Port = 67

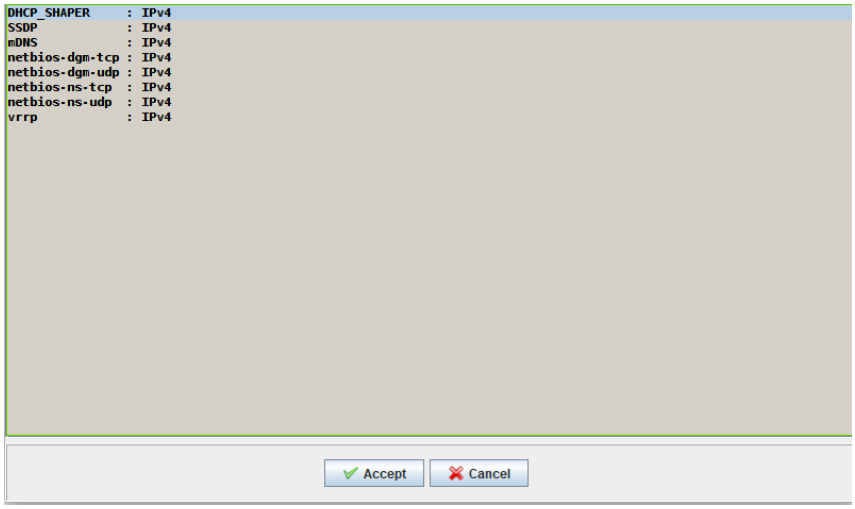



When the class is created, select Client.QoS Policy.Map and add a policy ("Add Policy" button).

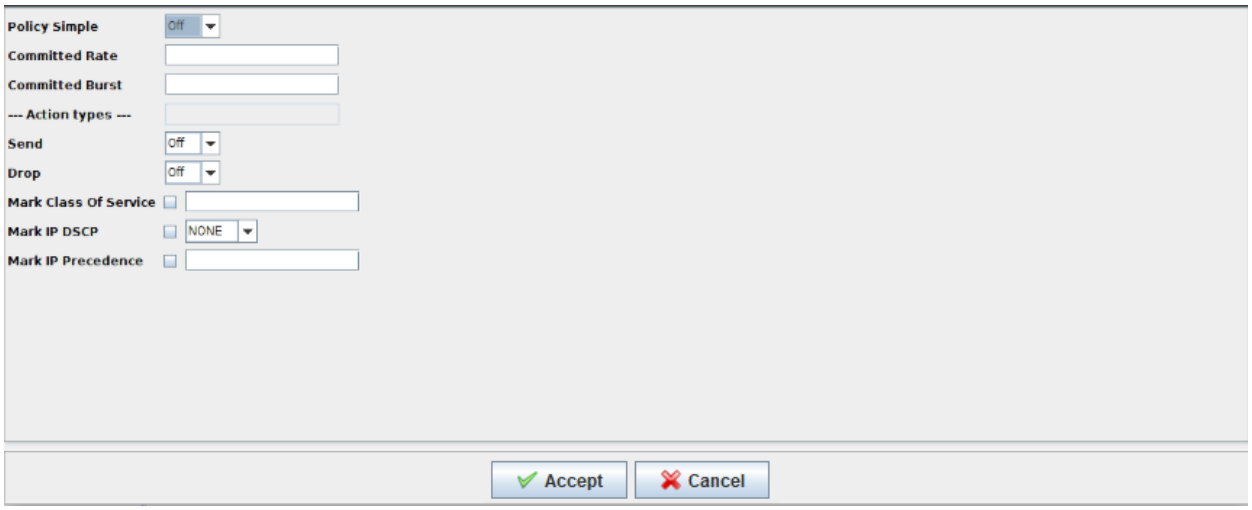



Then add the class to the policy.
To do that, select the class and click "Add Class" button.

```
63
Host is up (0.00056s latency).
PORT     STATE         SERVICE
```




After that, specify limits and action in the opened window.



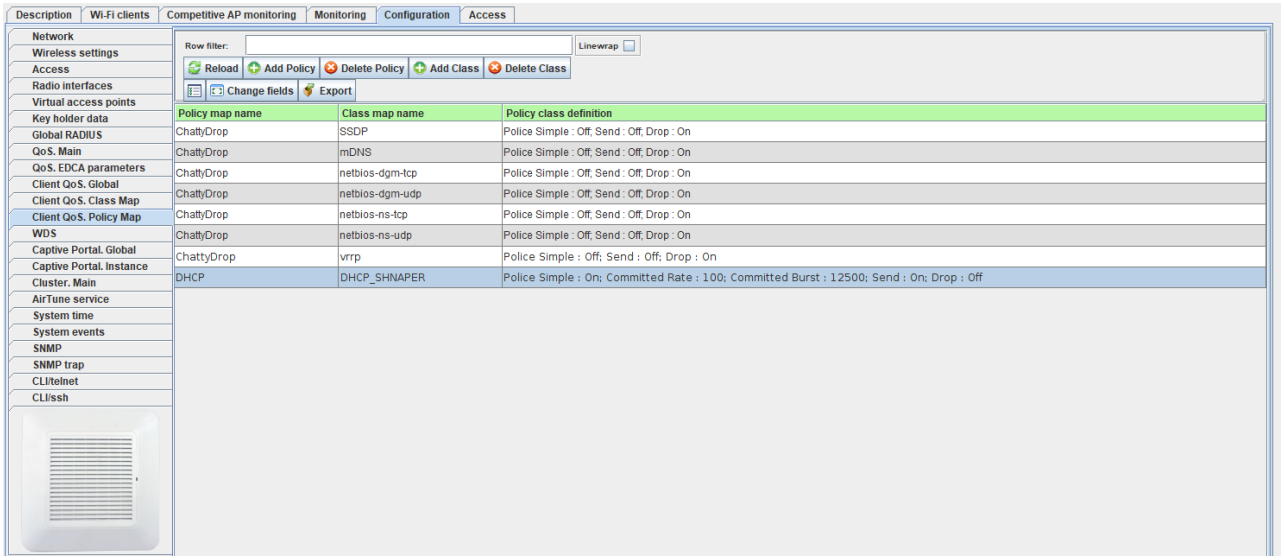

Policy Simple is a simplified setting where two parameters are defined:

- Committed Rate — the bandwidth guaranteed for matching traffic.
- Committed Burst — the maximum packet size in bytes that conforms the amount of traffic sent. It should ideally be 1.5 times higher than Committed Burst in bytes to work correctly.

The action performed on the traffic should be selected in Action types.
Send — if set to On, all packets of corresponding traffic flow will be transmitted;
Drop — if set to On, all packets of corresponding traffic will be dropped.

Only the traffic with certain speed should be transmitted, the rest of the packets should go to Drop. Consequently, enter the values and set Send to On.


The result will be a rule limiting DHCP traffic to 100 kbps.




When configuring a shaper on ESR, either Discover (from client to server) or Offer (from server to client) transmitting may be limited.

1. Limiting DHCP Discover transmitting from client to server

```
security zone-pair any self
  rule 999
    action permit
    rate-limit pps 2
    match not fragment
    match protocol udp
    match destination-port DHCP
    enable
  exit
exit
```

2. Limiting DHCP Offer transmitting from server to client

```
security zone-pair apuser any
  rule 999
    action permit
    rate-limit pps 2
    match not fragment
    match protocol udp
    match destination-port DHCP
    enable
  exit
exitt
```

## v1.14_Setting daily limit for BRAS (EN)


- Description
- Creating URL lists
    - Creating a welcome list
    - Creating white_list
- Creating services
    - Creating limit2h1Gb service
    - Creating the blocking service
- Creating a PCRF scenario
    - Creating a limit scenario
- Creating a tariff
    - Creating a limitTP tariff
- CheckCronBrasVerticle update interval
- How it works
- Constraints

## Description

**Problem**: a client should be provided with an opportunity to use a service for 2 hours on weekdays and download 1 Gb of traffic within the allotted time. Access should be denied when time or traffic quota is exceeded. Block should be cancelled at 7:00 (a client's timezone), a client is in Yekaterinburg. When access is blocked, https://eltex-co.com should be available. Other HTTP/HTTPS requests should be redirected to "Access denied" page.
To solve the problem, PCRF scenarios should be used. A scenario is a sequence of services. Services used in a scenario should be finite and have a condition for transition to next step.
A condition may be:

- common time or traffic limit, upon the exceeding of which a user is switched to next step of the scenario;
- cron limit — an expression in quartz cron format that contains the time at which a user should be switched to next step.

In scenario settings, again reserved word is available. It means a user should go back to the beginning and continue getting a service. In this case, limits on specific steps are set again.
SoftWLC and BRAS are assumed to be configured and put into operation.

> Software version:
>
> SoftWLC 1.13
> PCRF license is required for scenarios to work correctly
> ESR 1.6.2

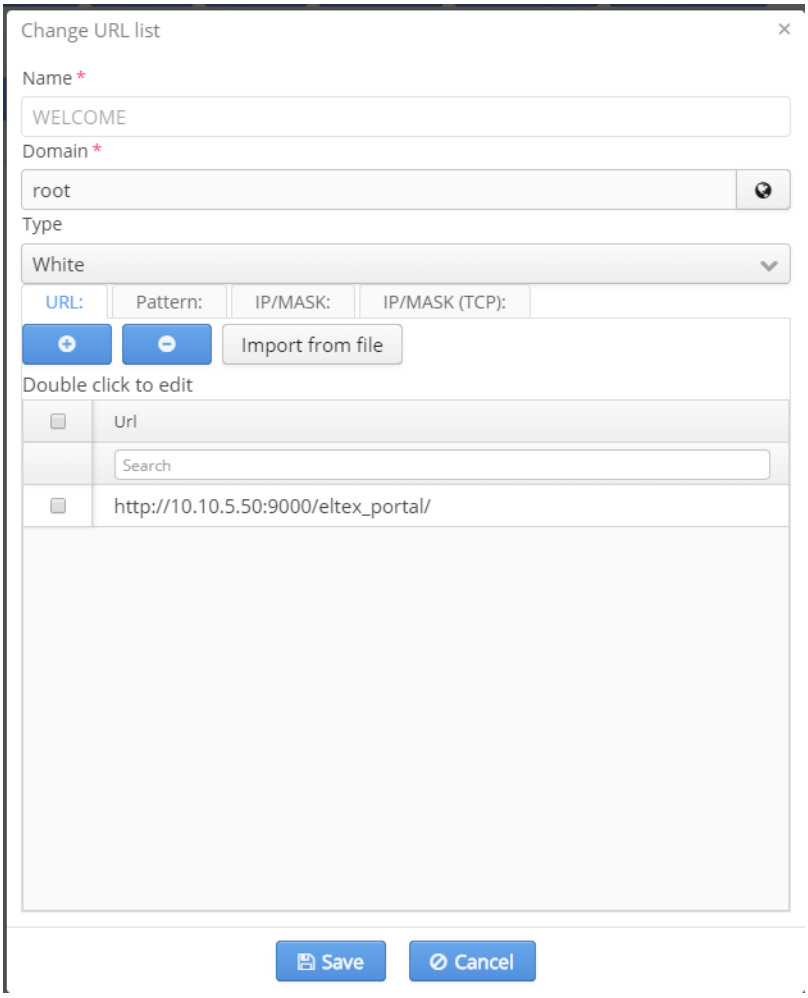
## Creating URL lists

To solve the problem, two lists should be created: welcome and white_list. Welcome list is used during client re-authorisation and created when the initial SoftWLC setting is done to work with BRAS.
Select PCRF settings → URL lists tab in the Admin Panel.

### Creating a welcome list

The list should contain the address of the portal

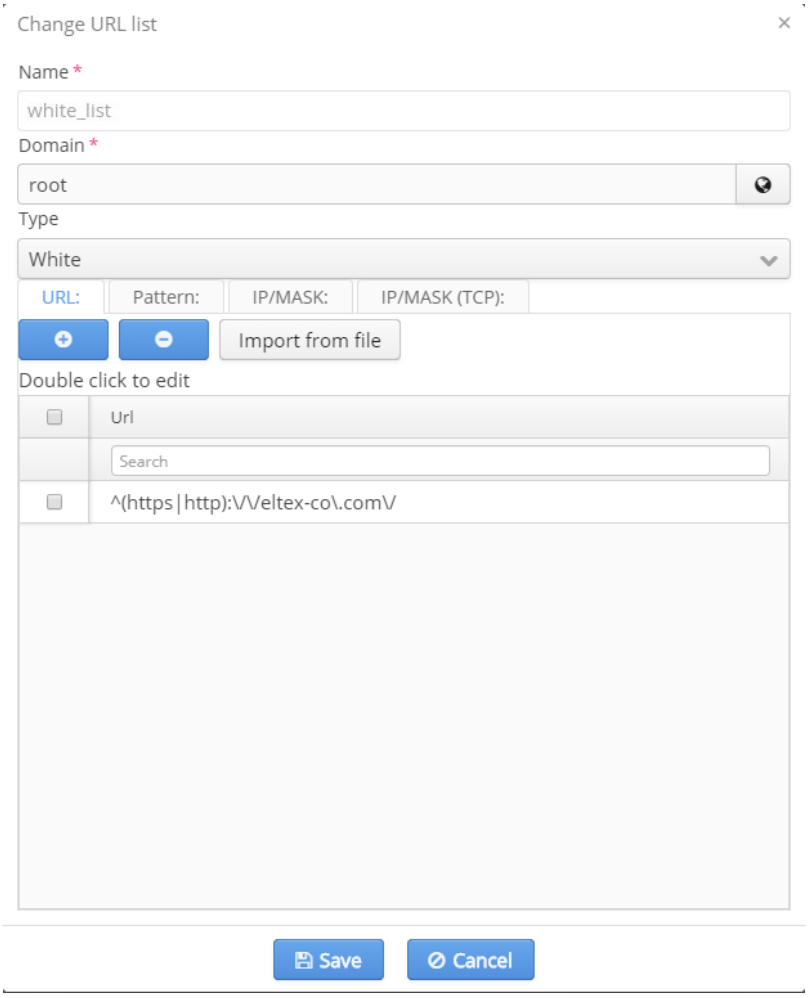
```
http://10.10.5.50:9000/eltex_portal/
```




### Creating white_list

The list should contain the address of the resource that will be available when access is blocked. For convenience, enter the address as a regular expression

```
^(https|http):\/\/eltex-co\.com\/
```

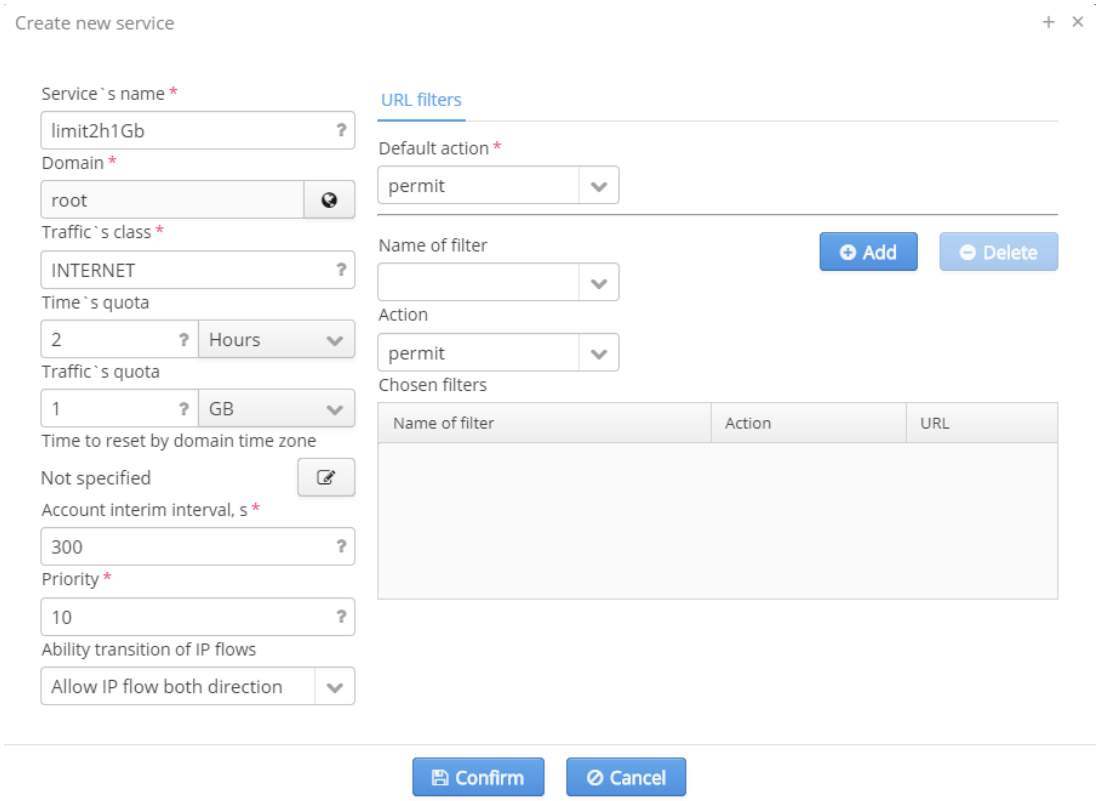



## Creating services

Select Services and tariffs → PCRF services in the Admin Panel

### Creating limit2h1Gb service

The service will be the 0th step of our scenario**.** Set Time's quota and Traffic's quota in accordance with the problem statement



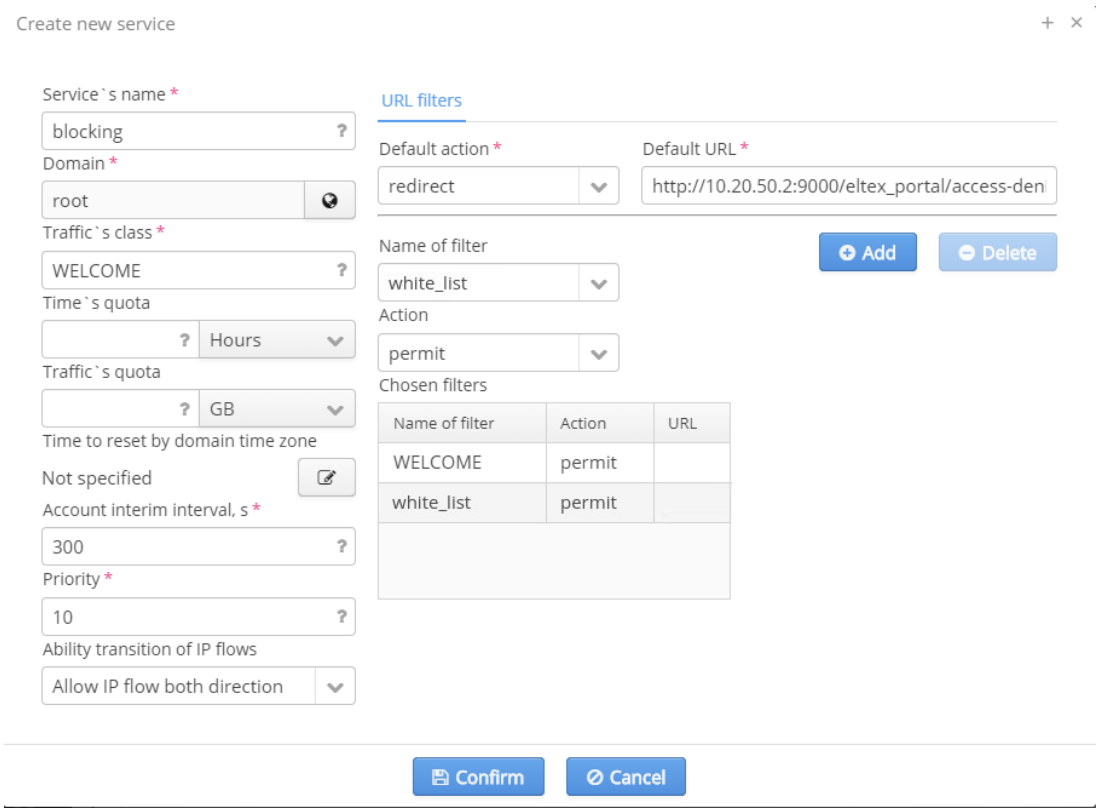

- Traffic's class — INTERNET, the class should allow access via any protocol;

```
ip access-list extended INTERNET
  rule 10
    action permit
    enable
  exit
exit
```

- Time's quota — 2 hours according to the problem statement;
- Traffic's class — 1 Gb according to the problem statement;
- Account interim interval — 300 seconds;
- Priority — 10, services with a lower number are processed first;
- Default action — permit.

### Creating the blocking service

The service will be the first step of our scenario. The service will block Internet access, all HTTP/HTTPS requests will be redirected to "Access denied" page, https://eltex-co.com/ will be accessible via HTTP/HTTPS.




- Traffic's class — WELCOME, the class allows access for interfaces that are proxied on BRAS

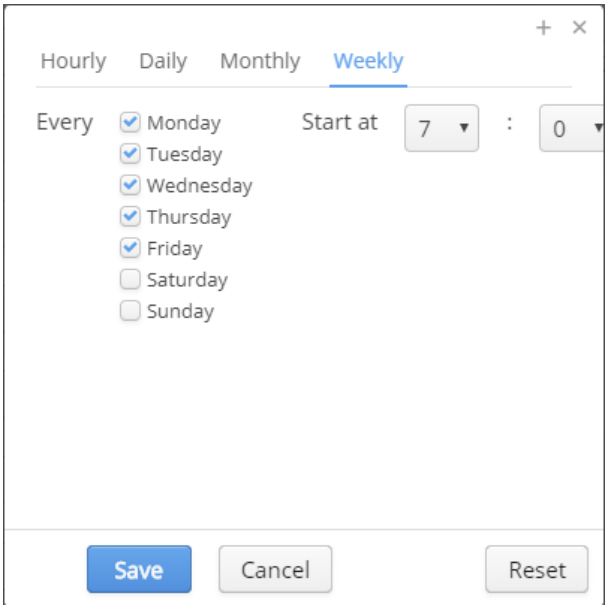
```
ip access-list extended WELCOME
  rule 1
    action permit
    match protocol tcp
    match destination-port 443
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match destination-port 8443
    enable
  exit
  rule 3
    action permit
    match protocol tcp
    match destination-port 80
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port 8080
    enable
  exit
  rule 5
    action permit
    match protocol tcp
    match destination-port 9000
    enable
  exit
exit
```

Account interim interval — 300 seconds;

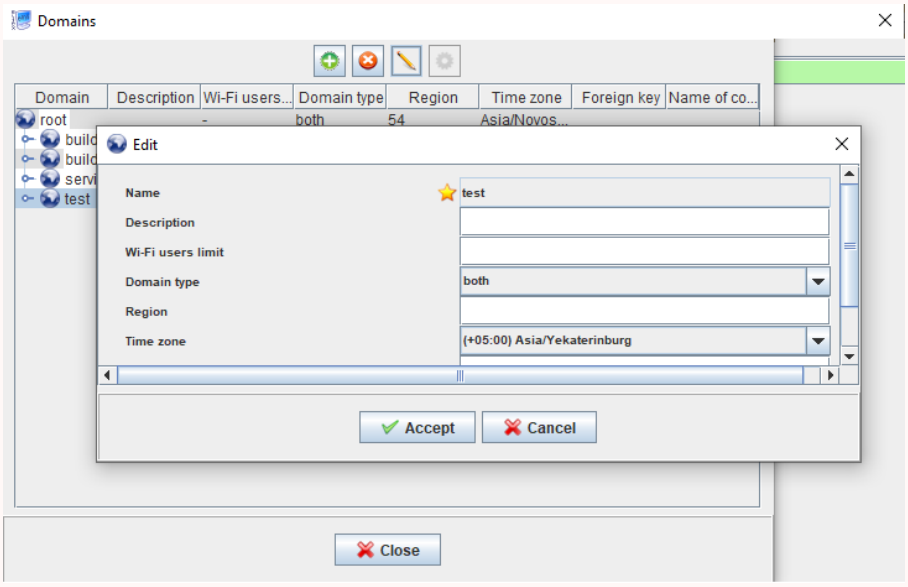
- Priority — 10, services with a lower number are processed first;
- Default action — redirect;
- Default URL — http://<ip address>:9000/eltex_portal/access-denied.jsp, a link to "Access denied" page. Custom page may be created with the help of the v1.14_Portal Constructor (EN).

Add URL filter with Permit action and a welcome URL list. This filter is used to allow access to "Access denied" page.
Add URL filter with Permit action and a white_list URL list. This filter is used to allow access to https://eltex-co.com

In the additional menu  set block cancellation time




Block reset takes into account a client's timezone that should be defined in EMS service domain settings. If a timezone is not defined in a client's domain, a bottom-up tree search will be conducted. If a timezone is not found in parent domains, block reset will take UTC ± 0:00. Timezone is set in EMS domain settings

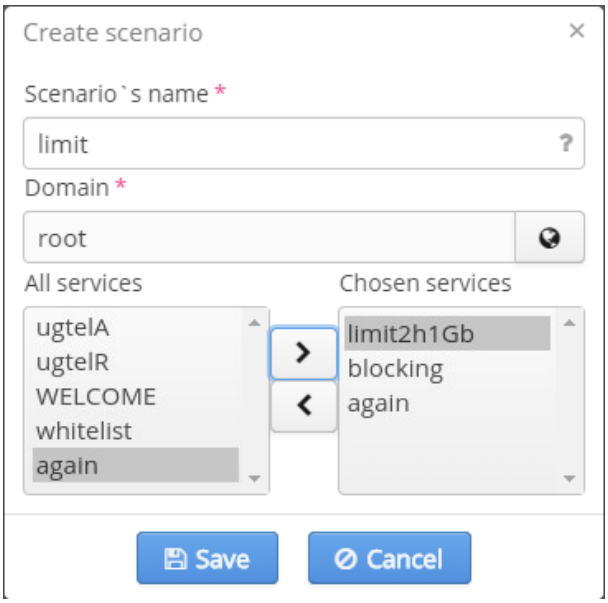



## Creating a PCRF scenario

Select Services and tariffs → PCRF scenarios tab in the Admin Panel.

### Creating a limit scenario

Add the created services to the scenario, the services will be displayed from the top down



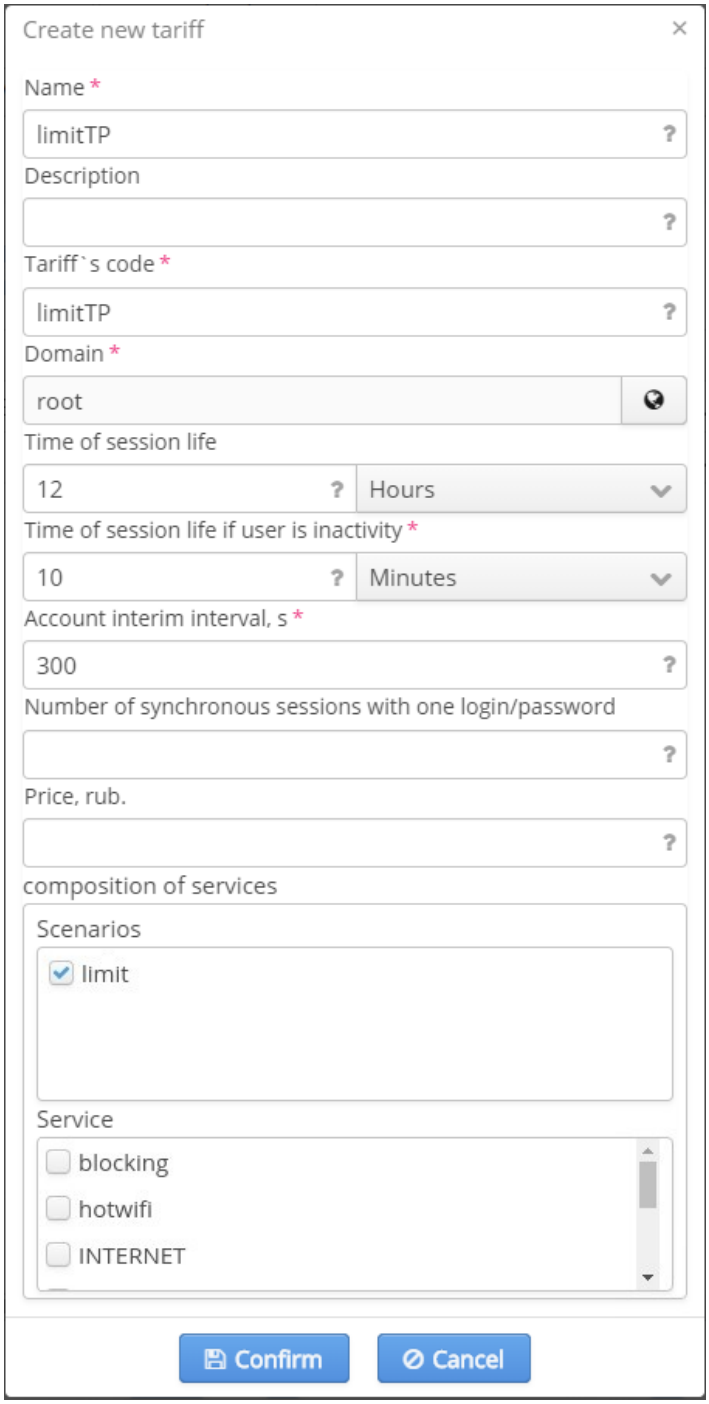

At the zeroth step, a client gets the service with quota (limit2h1Gb). When quota is exceeded, the first step with the blocking service will be available. The service will be operating until the reset. After the reset, a client moves to the second step and switches back to the zeroth one.

## Creating a tariff

Select Services and tariffs → Tariffs tab in the Admin Panel, change the filter to PCRF/BRAS

### Creating a limitTP tariff

Add a new tariff and select a previously created limit scenario




- Name — limitTP;
- Tariff's code — may be the same as Name;
- Domain — since a tariff is applicable for different clients, it should be created in root domain;
- Time of session life — set a session validity period on BRAS. If a client's session is terminated due to the end of Time of session life, and a client is active at the moment, the current session will be terminated, and a new session will start. The client will be authorized via mac-auth;
- Time of session life if user is inactive — when this period of inactivity is ended, a client is considered as disconnected one, and the session is terminated.

- Account interim interval — 300 seconds;
- Scenarios — select a previously created scenario.

When a tariff is created, it should be assigned to a client's portal. For L2, a portal is selected in PCRF settings → L2 subnets tab of the Admin Panel. For L3, a portal is selected in EMS (SSID Manager).

## CheckCronBrasVerticle update interval

CheckCronBrasVerticle update interval is set in bras.cron.update.interval block of PCRF configuration

```
"bras.cron.update.interval": {
  "interval" : 1,
  "unit": "hours"
},
```

Default update interval is 1 hour, in order to increase the number of checks, change the parameter and restart PCRF. For example, to update every 1800 seconds:

```
"bras.cron.update.interval": {
  "interval" : 1800,
  "unit": "Seconds"
},
```

## How it works

A client passes the registration and gets a configured scenario. To see which step a client is at and which services does he have, Mongo can be used:

```
> use pcrf
switched to db pcrf
> db.scripts.find({"user_name" : "79139001234"}).pretty();
{
        "_id" : "5d0c9359cc4e0c72ceb395ff",
        "domain" : "Auto1_test.Sibir.OTT.root",
        "title" : "limit",
        "user_name" : "79139001234",
        "step" : 0
}
> db.service.find({"user_name" : "79139001234"}).pretty();
{
        "_id" : "5d0c9359cc4e0c72ceb39600",
        "user_domain" : "Auto1_test.Sibir.OTT.root",
        "user_name" : "79139001234",
        "service_list" : {
                "limit2h1Gb" : {
                        "service_domain" : "root",
                        "quota_time" : NumberLong(7200),
                        "quota_volume" : NumberLong(1073741824)
                },
                "blocking" : {
                        "service_domain" : "root",
                        "quota_cron" : "06/24/2019 - 07:00:00 YEKT"
                }
        }
}
```

The client is at the first step of a scenario including 2 services: limit2h1Gb and blocking. Two ways are possible:

- If a client's quota is exceeded, PCRF will send a CoA request (command=services-reauth) to BRAS and switch a client to the next step of the scenario. BRAS will request services from PCRF and get data on the new step. The step number in Mongo scripts collection will be changed; the quota for limit2h1Gb service will be set again.
  **scripts**

```
> db.scripts.find({"user_name" : "79139001234"}).pretty();
{
        "_id" : "5d0c9359cc4e0c72ceb395ff",
        "domain" : "Auto1_test.Sibir.OTT.root",
        "title" : "limit",
        "user_name" : "79139001234",
        "step" : 1
}
```

- If a client's quota is not exceeded, and a client is disconnected from the network, his session will be terminated after 10 minutes, i.e. he will remain at the zeroth step of the scenario.

At the scheduled time, PCRF will review data in the service collection. If a client is at the zeroth step, PCRF will reset quota to an initial state; if a client is at the first step, PCRF will switch him to the next step, as a reserved word is "again". PCRF debug logs may contain the following lines:

```
==> /var/log/eltex-pcrf/eltex-pcrf-service.log <==
2019-06-21T16:09:16,955 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:).
Current time 2019-06-21T09:09:16.955Z
2019-06-21T16:09:17,070 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:).
Imagine time 06/21/2019 - 14:09:00 +0500
2019-06-21T16:09:17,071 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:). Value
{"quota_cron":"06/21/2019 - 14:09:00 +0500","service_domain":"root"}
2019-06-21T16:09:17,071 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:).
service_name blocking, cronTime 2019-06-21T14:09+05:00, service_domain root
2019-06-21T16:09:17,071 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:).
Difference 16
2019-06-21T16:09:17,071 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:). Start
to cron BrasCron(userName=79139001234, userDomain=Auto1_test.Sibir.OTT.root,
serviceName=blocking, date=2019-06-21T14:09+05:00[Asia/Yekaterinburg], serviceDomain=root)
2019-06-21T16:09:17,076 [vert.x-eventloop-thread-1] DEBUG ReinitAllSerPersExcCronStrg ?.(line:).
Search sessions by name = '79139001234' AND domain = 'Auto1_test.Sibir.OTT.root' for all
services: []
2019-06-21T16:09:17,076 [vert.x-eventloop-thread-1] DEBUG ReinitAllSerPersExcCronStrg ?.(line:).
Try to get tariff domain for service name=79139001234, domain=Auto1_test.Sibir.OTT.root. Reload
from base 25, hashed 41997.
2019-06-21T16:09:17,084 [vert.x-eventloop-thread-2] DEBUG CheckCronBrasVerticle ?.(line:).
Successfully all checked
```

The step number in scripts collection has changed:

```
> db.scripts.find({"user_name" : "79139001234"}).pretty();
{
        "_id" : "5d0c9359cc4e0c72ceb395ff",
        "domain" : "Auto1_test.Sibir.OTT.root",
        "title" : "limit",
        "user_name" : "79139001234",
        "step" : 2
}
```

When a client returns, updated services consistent with the problem stated will be available for him.

## Constraints

If there are two or more services with quota within a scenario, and a client has not reached the blocking service, he will remain at the current service with quota, i.e. he will not be switched to the zeroth step.

Once a client is reconnected, a service will not be fully provided, as the work will start from the mid-way point.

## v1.14_Creating dynamic tunnels using ESR location configuration in a client node (EN)


- General description
- The classic scheme of node tree search for data tunnel establishment
- Problems of defining an ESR for data tunnel establishing in a classic ESR search
- The scheme of searching ESR for data tunnel establishment by location configuration in a node
- Configuring ESR location in EMS
- Occupancy monitoring of the node where ESR devices for data tunnel establishment are located
- ESR location configuration principles


# General description

According to the classic implementation, the search of an ESR to which a command for data tunnel establishment (data tunnel create) should be sent, is conducted up to the node tree beginning with a node where an AP is located. This logic requires AP and ESR to be located at the same branch of ESR object tree, and ESR to be located at the same node with AP or higher. This solution is not suitable for clients that have a part of access points grouped by clients and another part grouped by regions in its domain structure. It is not also suitable for federal clients that have division into clients (AllClients.Federal.BANK) and then into regions (BANK.Centr.Moskva).

The proposed solution gives an opportunity to configure the ESR location parameter "Domain of Station ESR" where a node where a search for an ESR (for data tunnel establishment) should be conducted can be specified. Thus, when moving up the tree from an AP to find an ESR for data tunnel establishment, EMS will be able to use this parameter to move from a federal client node to a region node containing the ESR.

> It should be understood that a data tunnel can be established only to the ESR used for AP management tunnel. An AP decides what termination addresses should be used to establish 43-option GRE from a DHCP server when receiving a primary address - EMS configuration has no effect! Therefore, the engine to search ESR devices appropriate for data tunnel establishment assumes that ESR devices to which an access point will establish (or has already established) a management tunnel will be found as a result.

## The classic scheme of node tree search for data tunnel establishment

ESR has two options to establish data tunnels for access points:
1) data tunnels configured dynamically (locally) - in this case, all necessary information for data tunnel configuring is contained in ESR configuration, and its interaction with EMS management system is not required (this option is not considered further);
2) data tunnels configured dynamically on RADIUS server commands. In this case, it is necessary to configure interaction with the RADIUS server on ESR and complete the settings in EMS. PCRF server acts

as a RADIUS server with which ESR interacts. This way to establish data tunnels will be considered further.

Establishing data tunnels to ESR is made on the PCRF command initiated by EMS and sent in the following cases:

1) initializing a new AP;
2) reinitializing of an AP;
3) moving an AP to another node;
4) changing SSID parameters linked to a domain where an AP is located;
5) removing/creating a SSID link to an AP domain;
6) changing/assigning/removing a domain shaper or SSID of an AP.

In all these cases, EMS should define ESR devices to which a command for data tunnel establishment will be sent. To use ESR for data tunnel establishment, it should be added to EMS node tree with "ESR mode" = "Station" in the tab "Access". It should not be phased out.

> To successfully establish tunnels on ESR, it is necessary to have a configured location in SSID settings. This location should be the same as the location configured on ESR clients' bridge to which a data tunnel should be established.

According to classic logic for searching the ESR to which data tunnels will be established, EMS will start with checking the node where an AP is located for ESR devices suitable for data tunnel establishment. If such a device has not been found, EMS will continue its search in a higher-level node and so on, until an appropriate ESR is found, or the root is reached (EMS node). In case if ESR has not been found, the command for data tunnel establishment will not be executed. An example of the mechanism work can be seen in Figure 2.1.

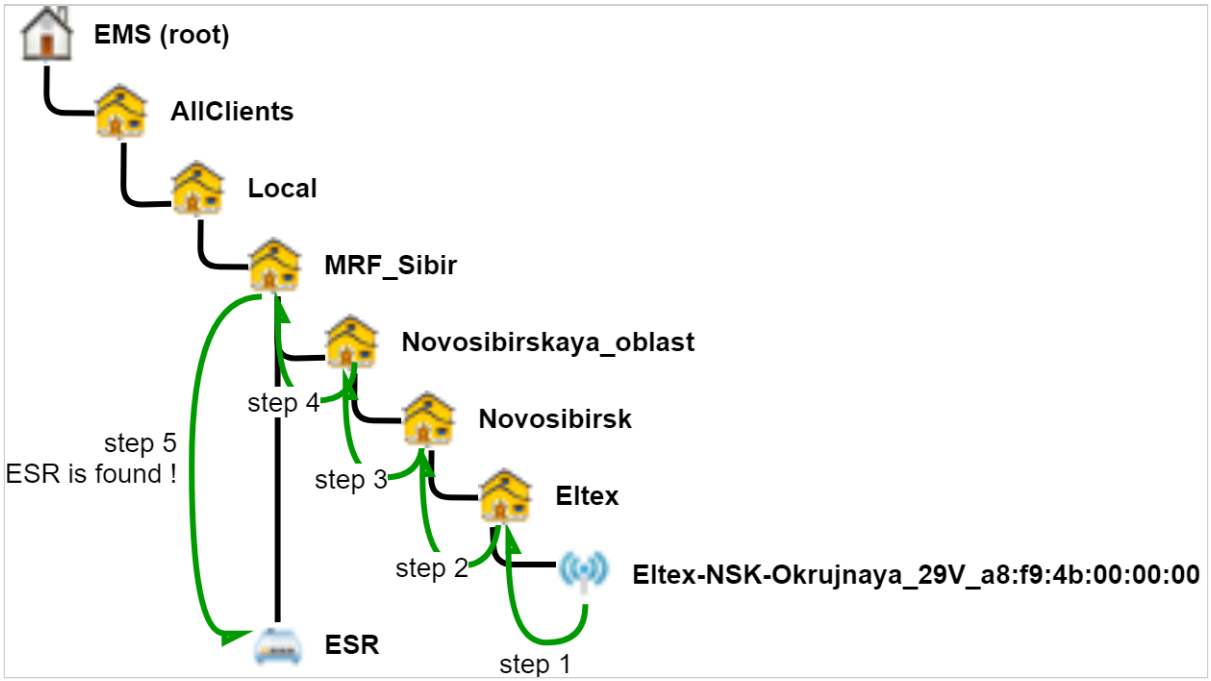



Figure 2.1

step 1: An AP is detected in Eltex node;
step 2: The node "Eltex" is checked for the ESR. It is not found, the algorithm moves to the higher-level node "Novosibirsk".
step 3: The node "Novosibirsk" is checked for the ESR. It is not found, move to the higher-level node "Novosibirskaya_oblast";
step 4: The node "Novosibirskaya_oblast" is checked for the ESR. It is not found, the algorithm moves to the higher-level node "MRF_Sibir";
step 5: The node "Novosibirskaya_oblast" is checked for the ESR. It is found! It will be used for data tunnel establishment.

If several ESR devices appropriate for data tunnel establishment are found, the command will be sent to all of them.

## Problems of defining an ESR for data tunnel establishing in a classic ESR search

Look at the scheme in Figure 3.1:

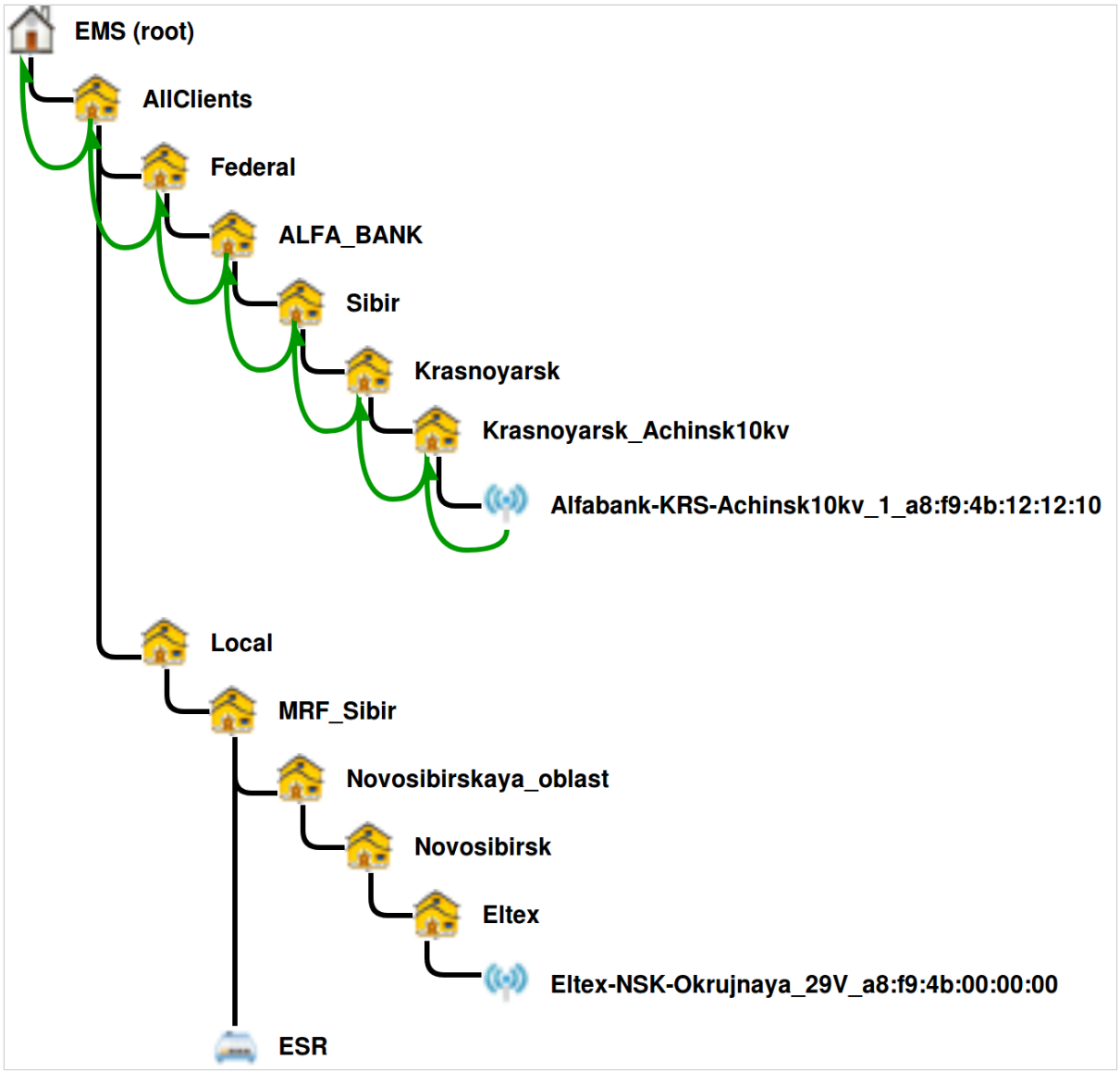



Figure 3.1

In the scheme for AP Alfabank-KRS-Achinks10kv_1_a8:f9:4b:12:12:10 given above, a data tunnel should be established from the node "Krasnoyarsk_Achinsk10kv" to the ESR that is located in the node "MRF_Sibir". If the classic scheme is used, the device will not be detected, and the command for data tunnel establishment will not be sent. To solve this problem, the opportunity to define ESR location in node settings has been added to SoftWLC 1.14 and EMS 3.18. ESR search logic for tunnel establishment has been also added.

## The scheme of searching ESR for data tunnel establishment by location configuration in a node

In the scheme of searching ESR for data tunnel establishment by location configuration there is an opportunity to specify a domain to search an ESR in node configuration. The logic is as follows:

1) EMS starts checking an AP node for configuration of a domain appropriate to move to. This rule has the highest priority, and if the domain is found, EMS will move to it regardless of whether there is an ESR suitable for data tunnel establishment. 2) if a transition rule for moving to another node has been found, the node is checked for ESR searches held before:

2.1) if the search has not been held, the algorithm will move to this node, and start checking for the transition rule (beginning from paragraph 1);

2.2) if the search has been held, the rule is ignored, and the algorithm moves to paragraph 3.

3) if a transition rule had not been found (or it was ignored due to the reasons described in 2.2), a search to find ESR devices appropriate to establish a data tunnel will be done;

4) if no transition rules and ESR devices for data tunnel establishment had been found, the algorithm moves to a higher-level node, and the search is done again, beginning with paragraph 1.

In Figure 4.1, a block diagram of the algorithm for searching an ESR appropriate for data tunnel establishment is given:

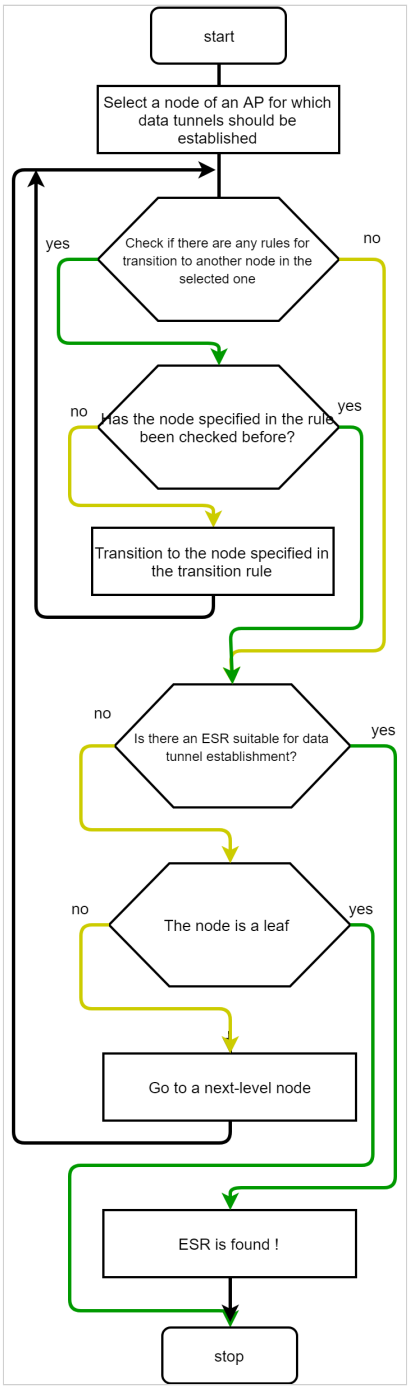



Figure 4.1

The below Figure 4.2 shows an example of search implementation for the case when a domain node contains a rule of transition to another domain to find ESR for data tunnel establishment:

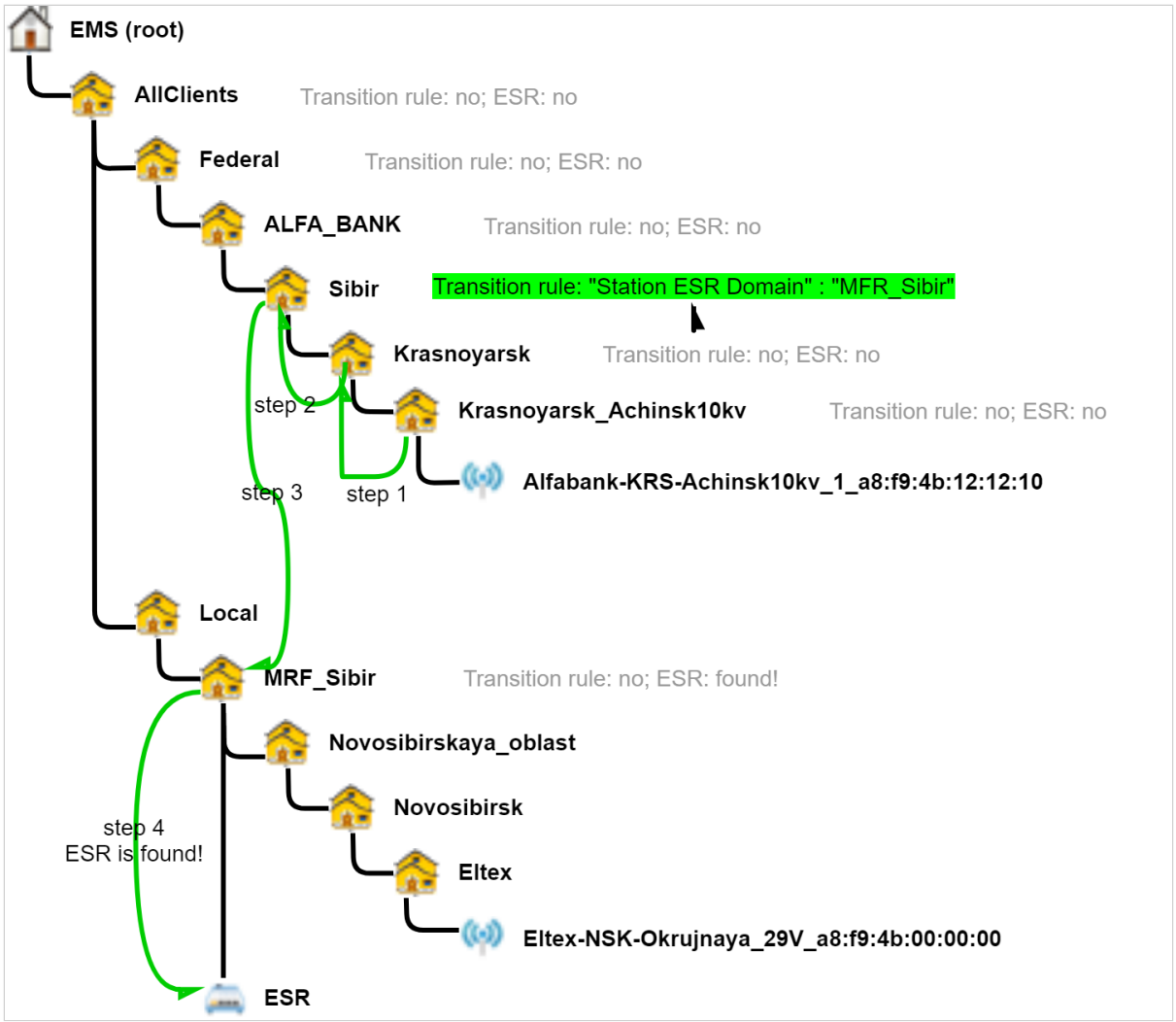



Figure 4.2

step 1: check the node Krasnoayarsk_Achinsk10kv for the transition rule: not found; check the node for ESR devices appropriate for data tunnel establishment: not found; move to the next node Krasnoyarsk;

step 2: check the node Krasnoyarsk for the transition rule: not found; check the node for ESR devices appropriate for data tunnel establishment: not found; move to the next node Sibir;

step 3: check the node Sibir for the transition rule: found, points to the node MRF_Sibir; move to this node (after verifying that there were no transitions to it before);

step 4: Check the node MRF_Sibir for the transition rule: not found; check the node for ESR devices appropriate for data tunnel establishment: ESR is found!

## Configuring ESR location in EMS

In the example in the figure 5.1. an AP is located in the node "Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root". ESR devices to which it establishes GRE tunnels according to option 43 parameters assigned during getting the primary address, are located

in the node "MRF_Sibir.Local.AllClients.root". Therefore, it will not be found by the AP, if the classic ESR search will be done. It is necessary to define a node on which ESR location will be configured, and from which a transition to a node containing ESR will be made.

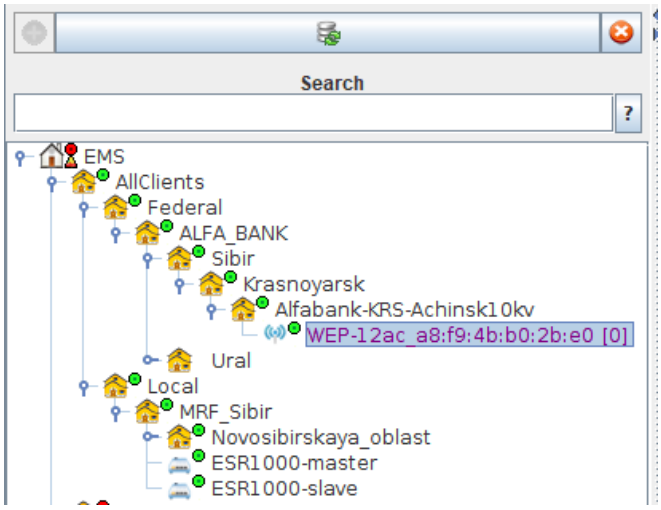



Figure 5.1

In the example above (Figure 5.1), ESR location could be configured in the node "MRF_Sibir.Local.AllClients.root", but it would not be appropriate, as the rule would work only for access points that are located in this node and in lower-level ones. When new clients will be connected, new nodes will be created for them in neighbouring branches. Thus, it will be necessary to define ESR location for each new client and to configure it for all existing clients in the transition to a scheme with dynamic configuration of data tunnels using RADIUS commands, that can be a very time-consuming task. But if a rule that will oblige all access points located lower than the domain "Sibir" to establish tunnels to ESR devices located in the node "MRF_Sibir" (and to take it into consideration when assigning a primary address to an AP) is adopted, then ESR location can be configured in the node "Sibir" (of the domain "Sibir.ALFA_BANK.Federal.AllClients.root"), that will allow all access points located lower than the node "Sibir" to find an ESR, to which data tunnels can be established without additional settings. To configure ESR location, move to the node "Sibir" and open the tab "Access" (Figure 5.2).

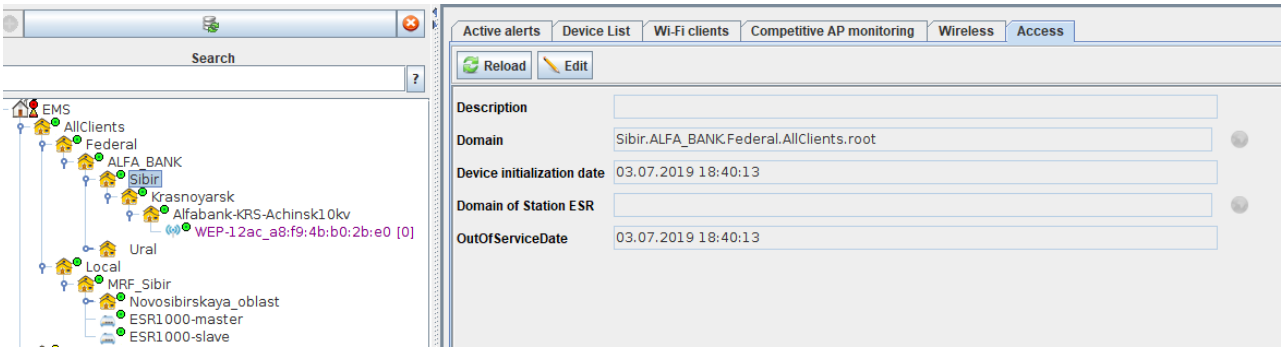



Figure 5.2

ESR location configuration is specified in "Domain of Station ESR". To change it, click "Edit" in the tab "Access" of the node. Edit window will be opened (Figure 5.3):

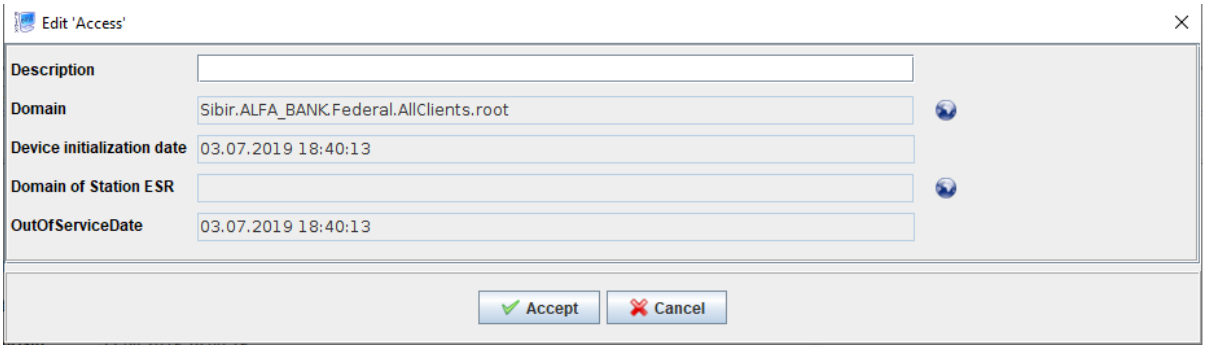



Figure 5.3

In the window, select ESR location by clicking a button  to the right of "Domain of Station ESR". Domain selection window, where a domain with node containing ESR to which an AP will establish tunnels, will be opened (Figure 5.4):

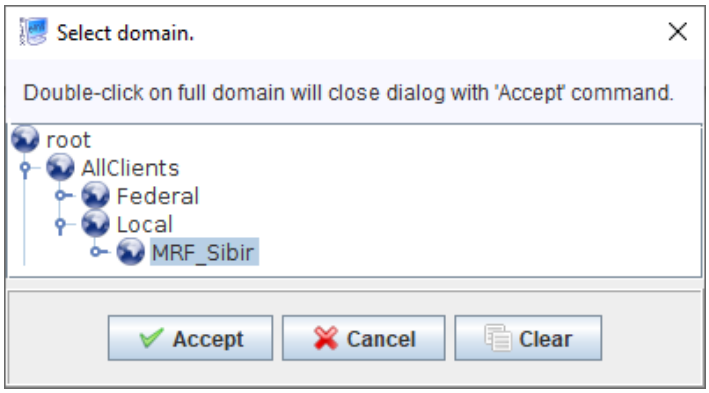



Figure 5.4

Click "Accept".

In "Domain of Station ESR", a transition rule will appear. The rule will contain a domain where a transition will be made to search ESR for data tunnel establishment (Figure 5.5).

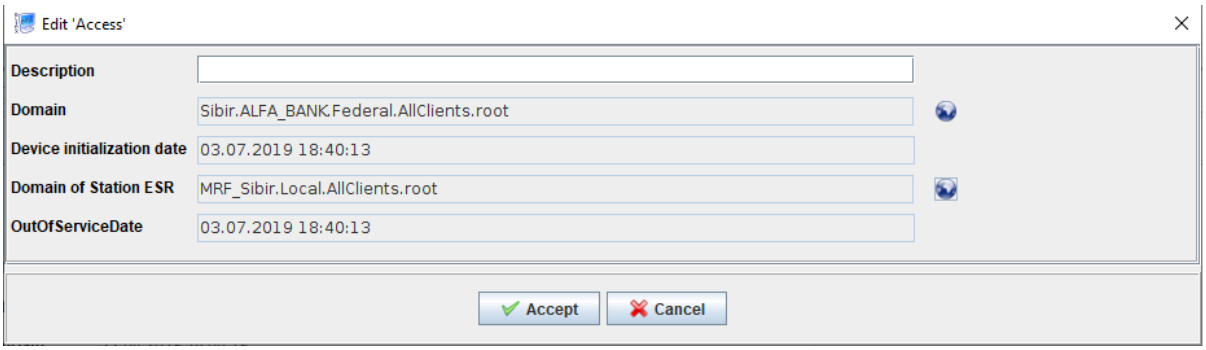



Figure 5.5

Click "Accept" to confirm the changes.

As can be seen in Figure 5.6, a domain to which a transition will be made when searching ESR for data tunnel establishment, will appear in the field "Domain of ESR Station" of the tab "Access".

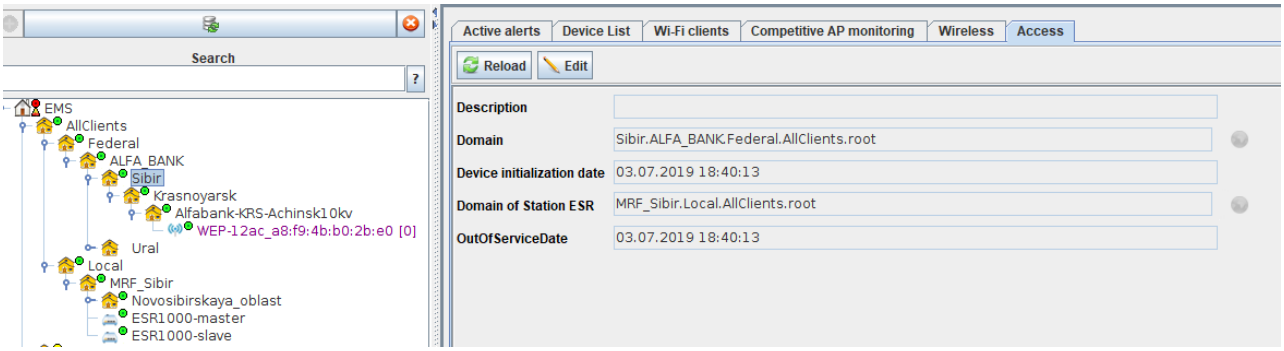



Figure 5.6

If a transition rule is adopted in a node (and in lower-level nodes) where access points initialized before are located, it is necessary to initialize them again (Figure 5.7).

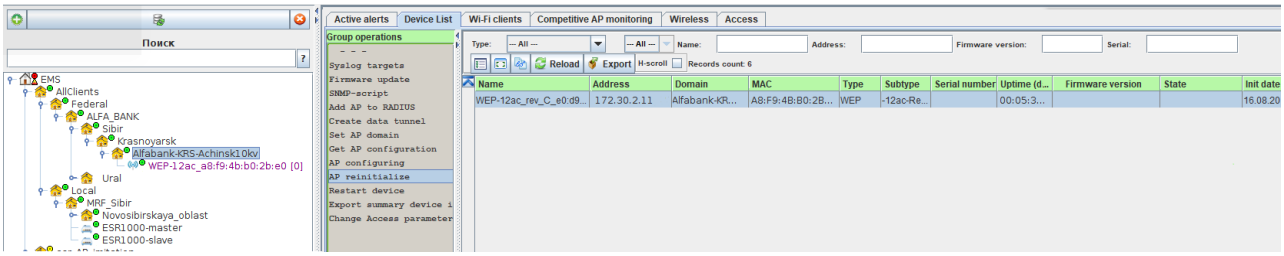



Figure 5.7

Perform AP reinitialization. During the process, the following entries can be seen in a log:

Station ESR objects for AP 172.30.2.1 have been found in MRF_Sibir.Local.AllClients.root

- ESR1000-slave 100.123.0.174

- ESR1000-master 100.123.0.173

Tunnel IP = "192.168.253.11"

Send a command 'data-tunnel create' to ESR NAS ip 100.123.0.174

Send a command 'data-tunnel create' to ESR NAS ip 100.123.0.173

This log demonstrates that ESR for data tunnel establishment has been successfully found, and the command for tunnel creation has been sent to it.

### Completely successful AP reinitialization log

12.07.2019 14:39:55 Reinitialization of AP 'WEP-12ac_a8:f9:4b:b0:2b:e0' (172.30.2.11)
12.07.2019 14:39:55 Reconfiguration of a wireless access point
Started for reinitialization of 'WEP-12ac_a8:f9:4b:b0:2b:e0'
initialization rule (found by 'MAC a8:f9:4b:b0:2b:e0')
ConfigurationTemplate = ;
FirmwareUpdateEnabled = false;
FirmwareUpdateProtocol = HTTP;
NEED_RESET = false;

RadiusApSecret = eltex;
SnmpReadonlyCommunity = public;
SnmpReadWriteCommunity = private;
SnmpTransportType = TCP;
TreeNodeDomain = Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root;
DeviceName = ;
KeyType = MAC;
KEY = a8:f9:4b:b0:2b:e0;

12.07.2019 14:39:56 Step 1: Updating access parameters
12.07.2019 14:39:56 Step 2: Checking RADIUS NAS
12.07.2019 14:39:56 Step 3: Firmware updating
12.07.2019 14:39:56 Firmware update is not required
12.07.2019 14:39:56 Step 4: Reset to default values
12.07.2019 14:39:56 Configuration reset is not required
12.07.2019 14:39:56 Step 5: Setting configuration parameters
12.07.2019 14:39:56 Configuration template is not specified, parameter setting is not required.
12.07.2019 14:39:56 Step 6: Install AP domain 'Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root' to 'WEP-12ac_a8:f9:4b:b0:2b:e0' (172.30.2.11)
12.07.2019 14:39:56 AP domain 'Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root' has been successfully changed to 'WEP-12ac_a8:f9:4b:b0:2b:e0' (172.30.2.11)
12.07.2019 14:39:56 Step 7: Creating a tunnel for AP WEP-12ac_a8:f9:4b:b0:2b:e0 (mng ip 172.30.2.11)
Station ESR objects 172.30.2.11 has been found in MRF_Sibir.Local.AllClients.root
- ESR1000-slave 100.123.0.174
- ESR1000-master 100.123.0.173
Tunnel IP = "192.168.253.11"
Send a command 'data-tunnel create' to ESR NAS ip 100.123.0.174
Send a command 'data-tunnel create' to ESR NAS ip 100.123.0.173
12.07.2019 14:39:56 Step 8: Configuring SSID
12.07.2019 14:39:56 List of links:
'i-alfa-10[ALFA_BANK.Federal.AllClients.root]@Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root',
'i-alfa-11[ALFA_BANK.Federal.AllClients.root]@Alfabank-KRS-Achinsk10kv.Krasnoyarsk.Sibir.ALFA_BANK.Federal.AllClients.root'.
12.07.2019 14:39:56 Step 8.1: Getting device configuration
12.07.2019 14:39:57 Step 8.2: Preparing SSID list
12.07.2019 14:39:57 SSID list:
'i-alfa-10 (Radio 1, 2.4Ghz)',
'i-alfa-11 (Radio 1, 2.4Ghz)'.
12.07.2019 14:39:57 Step 8.3: Disabling SSID without a link
12.07.2019 14:39:57 No SSID to disable
12.07.2019 14:39:57 Step 8.4: Verifying and correcting
12.07.2019 14:40:02 SSID 'i-alfa-10' is successfuly processed on Radio 1
12.07.2019 14:40:08 SSID 'i-alfa-11' is successfuly processed on Radio 1
12.07.2019 14:40:08 Configuration of 'WEP-12ac_a8:f9:4b:b0:2b:e0' (172.30.2.11) is successfully saved.
12.07.2019 14:40:08 AP configuration is completed

If errors of the following type occurred in the log:

Send a command 'data-tunnel create' to ESR NAS ip 100.123.0.175

PCRF NBI error: CoA request error on 100.123.0.175: Timeout: No Response from RADIUS Server

It demonstrates that a problem occurred while running a command for establishing a tunnel on this ESR.

The following message:

12.07.2019 15:04:14 Step 7: Creating a tunnel for AP WEP-12ac_a8:f9:4b:b0:2b:e0 (mng ip 172.30.2.11)

No ESR objects found for the AP 172.30.2.11

Tells that no ESR devices appropriate for tunnel establishment have been found. The message does not necessary demonstrate a problem, because when the scheme with dynamically configured data tunnels is used, it is not necessary to send the 'create' command to ESR.

To clear ESR location configuration, move to the node where it is configured, open the tab "Access"and click "Edit". Select a domain in the field "Domain of Station ESR" and click "Clear" (Figure 5.8 below):

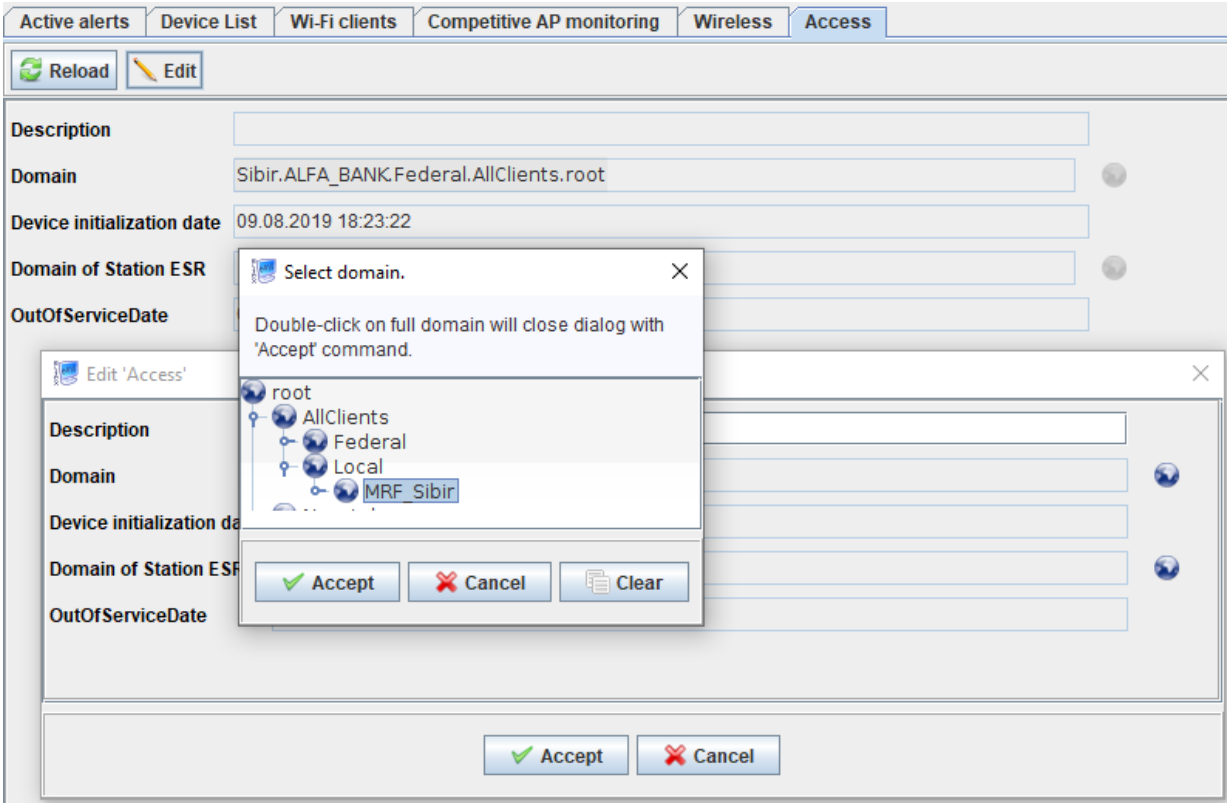



Figure 5.8

After that, configuration of "Domain of Station ESR" will be cleared (Figure 5.9):

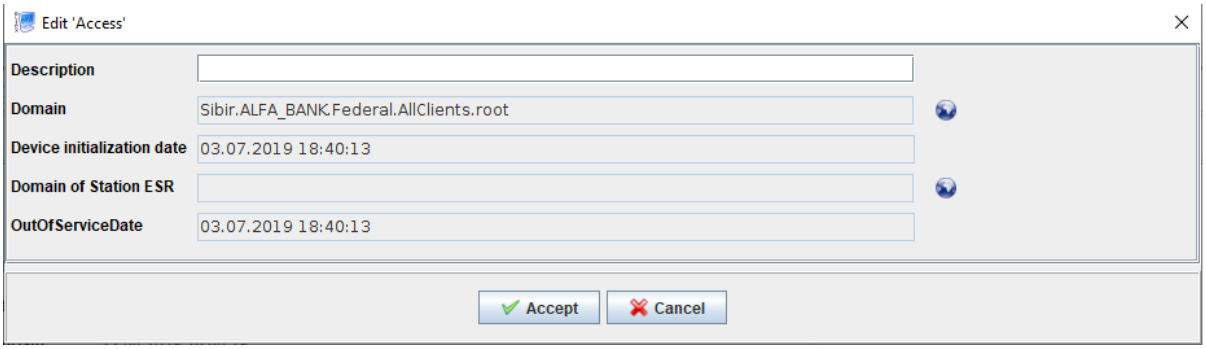
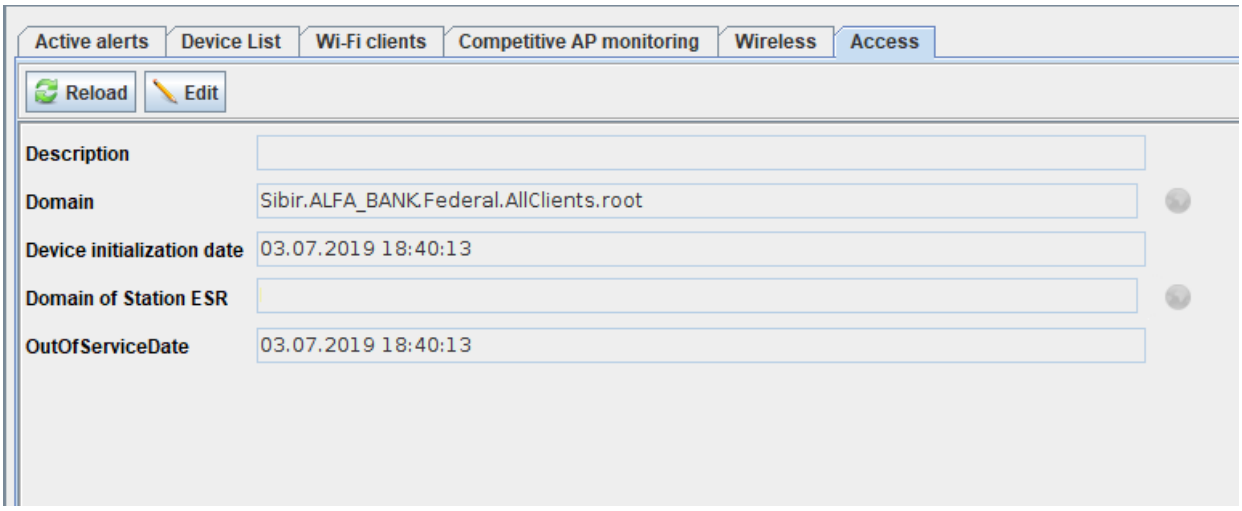



Figure 5.9

Click "Accept" to save configuration (Figure 5.10):




After that, a classic scheme will be used in this node to search for an ESR to which data tunnels can be established.

> Attention!!! Reinitialization is required for all access points that are located in the configured node or in lower-level nodes after assigning/changing/deleting ESR location in "Domain of Station ESR"!

## Occupancy monitoring of the node where ESR devices for data tunnel establishment are located

To monitor occupancy of nodes where ESR devices to which access points can establish tunnels, the new tab "Wireless" accessible for any node has been implemented. All ESR devices having access points that establish tunnels on them are displayed there, starting with the selected node and then down the tree.

In the example in Figure 6.1, the root node is selected to see all ESR devices:

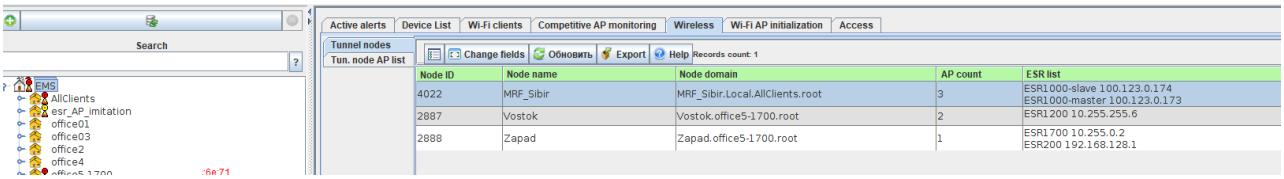



Figure 6.1

In Figure 6.1, in the tab "Wireless" → "Tunnel nodes" columns show:

- "Node ID" - object index
- "Node name" - the name of the node where ESR is located
- "Node domain" - the domain with the node where ESR devices are located
- "AP count" - the number of AP and ESR-10 that should establish tunnels on the ESR in the node. Attention! All devices that should establish tunnels are taken into account regardless of their accessibility. Phased-out devices are not taken into account (the checkbox "Out of service" in the tab "Access" is checked, or there is no tunnel ip).
- "ESR list" - the list containing ESR devices that are located in the node and can be used for data tunnel establishment. An indication that ESR data can be used for tunnel establishment is a setting in the tab "Access" → "ESR mode": "Station". Several ESR devices can be located in a node, because to provide redundancy, two devices are usually used. Attention! If there are no access points that can establish tunnels to ESR in a node, this not is not displayed!

To see a list of access points that build tunnels to specific ESR devices, select a node where these ESR devices are located and click "Tun. node AP list" in the left part of the tab "Wireless" (Figure 6.2).

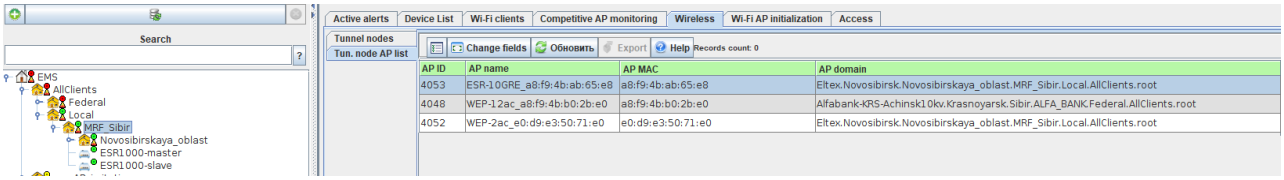



Figure 6.2

Columns in Figure 6.2 show:

- "AP ID" - object index
- "AP name" - object name
- "AP MAC" - MAC address of the device (AP or ESR-10)
- "AP domain" - the domain in which the device is located

All devices that should establish data tunnels to given ESR devices are displayed regardless of their accessibility. Only devices that have the status "Out of service" are not taken into consideration.
If there are no ESR devices to which data tunnels can be established, or there are no access points to establish them, nothing will be displayed in the tab.
For information to be displayed in the tab "Wireless", click "Edit privileges" in user roles configuration and check the "Dynamic tunnels" checkbox in the tab "WirelessCommon".

An opportunity to see a list of ESR devices to which a device (an AP or ESR-10) should establish tunnels is also implemented. To do this, select a device, open the tab "Monitoring" and select "Tunnel nodes" (Figure 6.3).

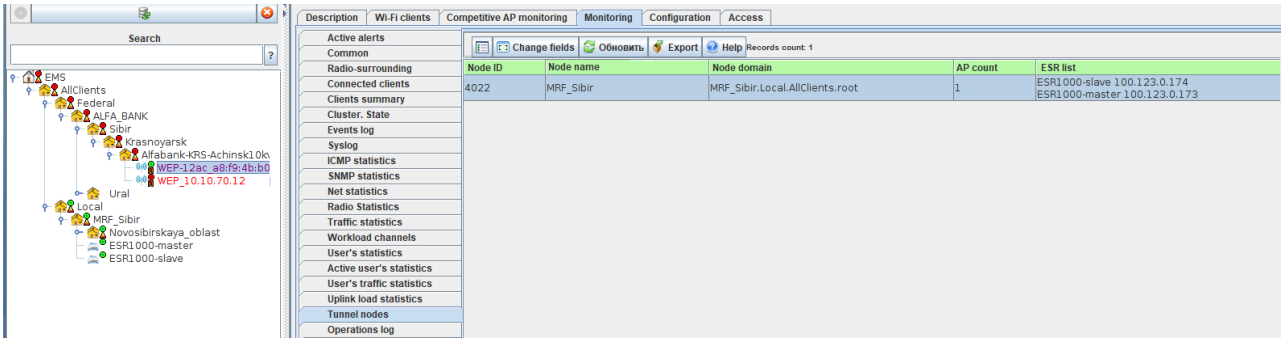



Figure 6.3

In the above figure 6.3, the following parameters are shown:
"Node ID" - object index
"Node name" - the node where an ESR device to which an AP should establish tunnels is located
"Node domain" - the domain in which ESR devices to which an AP should establish tunnels are located
"ESR list" - the list of devices that are located in the node. Several ESR devices can be located in a node, because to provide redundancy, two devices are usually used.

## ESR location configuration principles

When configuring ESR location, the following principles should be adhered to:

1. The node structure that does not allow using the classic search of ESR for data tunnel establishment (up the node tree from a node where an AP is located) should be avoided.
2. Never use the transition rule in a node where ESR devices appropriate for data tunnel establishment are located. In this case, ESR data will never be found.
3. Do not use several transition rules within one node branch from an AP to the root.
4. Do not use a double transition rule (a transition to the first node occurs, then the second transition rule is used in this node or in a higher-level node to move to the third node).
5. When configuring a transition rule, specify a node containing an ESR to which data tunnels are going to be established.

# v1.14_Troubleshooting Guide (EN)

## v1.14_Listing all cron events

The script is taken from github.com https://gist.github.com/Zitrax/3819487
We are grateful to the author Zitrax https://gist.github.com/Zitrax

The script parses crontab tasks for all system users and checks for active tasks in /etc/cron.
Run under the root user for correct execution.

**cronlist.sh**

```
#!/bin/bash

# System-wide crontab file and cron job directory. Change these for your system.
CRONTAB='/etc/crontab'
CRONDIR='/etc/cron.d'

# Single tab character. Annoyingly necessary.
tab=$(echo -en "\t")

# Given a stream of crontab lines, exclude non-cron job lines, replace
# whitespace characters with a single space, and remove any spaces from the
# beginning of each line.
function clean_cron_lines() {
    while read line ; do
        echo "${line}" |
            egrep --invert-match '^($|\s*#|\s*[[:alnum:]_]+=)' |
            sed --regexp-extended "s/\s+/ /g" |
            sed --regexp-extended "s/^ //"
    done;
}

# Given a stream of cleaned crontab lines, echo any that don't include the
# run-parts command, and for those that do, show each job file in the run-parts
# directory as if it were scheduled explicitly.
function lookup_run_parts() {
    while read line ; do
        match=$(echo "${line}" | egrep -o 'run-parts (-{1,2}\S+ )*\S+')

        if [[ -z "${match}" ]] ; then
            echo "${line}"
        else
            cron_fields=$(echo "${line}" | cut -f1-6 -d' ')
            cron_job_dir=$(echo  "${match}" | awk '{print $NF}')

            if [[ -d "${cron_job_dir}" ]] ; then
                for cron_job_file in "${cron_job_dir}"/* ; do  # */ <not a comment>
                    [[ -f "${cron_job_file}" ]] && echo "${cron_fields} ${cron_job_file}"
                done
            fi
        fi
    done;
}

# Temporary file for crontab lines.
temp=$(mktemp) || exit 1

# Add all of the jobs from the system-wide crontab file.
cat "${CRONTAB}" | clean_cron_lines | lookup_run_parts >"${temp}"
```

```
# Add all of the jobs from the system-wide cron directory.
cat "${CRONDIR}"/* | clean_cron_lines >>"${temp}"  # */ <not a comment>

# Add each user's crontab (if it exists). Insert the user's name between the
# five time fields and the command.
while read user ; do
    crontab -l -u "${user}" 2>/dev/null |
        clean_cron_lines |
        sed --regexp-extended "s/^((\S+ +){5})(.+)$/\1${user} \3/" >>"${temp}"
done < <((cut --fields=1 --delimiter=: /etc/passwd && find /home/ -maxdepth 1 -mindepth 1 -type d
-printf "%f\n") | sort | uniq)

# Output the collected crontab lines. Replace the single spaces between the
# fields with tab characters, sort the lines by hour and minute, insert the
# header line, and format the results as a table.
cat "${temp}" |
    sed --regexp-extended "s/^(\S+) +(\S+) +(\S+) +(\S+) +(\S+) +(\S+) +(.*)$/
\1\t\2\t\3\t\4\t\5\t\6\t\7/" |
    sort --numeric-sort --field-separator="${tab}" --key=2,1 |
    sed "1i\mi\th\td\tm\tw\tuser\tcommand" |
    column -s"${tab}" -t

rm --force "${temp}"
```

## v1.14_Troubleshooting of Wi-Fi users connections

**Initial diagnostics:**

1. Is an error repetitive or not? Duration. If an error occurred once and does not appear any more, a problem probably relates to a client's device.

2. On what AP (MAC address) was a problem found, what firmware version is installed on it? If a problem occurred on several access points, list all of them. If it is not possible, specify even a few access points.

3. On what SSID was a problem found (name, domain, auth type: without authorization, portal authorization, wpa-personal, wpa-personal+portal authorization, wpa-enterprise).

4. Client device type and model. If a problem is reproduced on devices of different types, make a list of all types and models.

5. Client device MAC address, login and domain.

**If a problem occurs again, further actions will depend on the authorization type:**

**1. Network without authorization (open)**

The points to be checked are listed below.

**A level of a signal from a client's device on an access point.**
If a signal level is -75 dB or lower, a client should get closer to an access point for this AP to "see" a client with a signal level -65dB.

**Does a client device receive an IP address?**
If an address is specified manually for a device, enable dynamic address obtaining.
If a device does not receive an address from a DHCP server, perform diagnostics of a DHCP server and network.

**If a device has an IP address, ping a default gateway and DNS servers.**

**2. Portal authorization**

The points to be checked are listed below.

**- A level of a signal from a client's device on an access point.**
If a signal level is -75 dB or lower, a client should get closer to an access point for this AP to "see" a client with a signal level -65dB.

**- Does a client device receive an IP address?**
If an address is specified manually for a device, enable dynamic address obtaining.
If a device does not receive an address from a DHCP server, perform diagnostics of a DHCP server and network.

> If a device has an IP address, but authorization process has not been completed, a gateway will not be pinged.

**- Check if redirection works correctly. Open your browser and try to access a website via http (not https!). For example,** http://www.sberbank.ru/**,** http://www.rostelecom.ru/**,** http://eltex-co.com/**.**

If redirection does not work, perform diagnostics. The instruction SoftWLC. Setting tariffs for portal authorization may help you.

**- Redirection works correctly when the address 8.8.8.8 is entered into the address bar.**

Check your local DNS server and if its address is transmitted to users via DHCP.

**- Redirection has worked, a user has been authorized but has not received an SMS with a password.**
If after registration on the portal a message "Data is being processed. Wait for an SMS to the entered number '79xxxxxxxxx' " is displayed, but waiting time is beyond 5 minutes, a message has been delivered to an SMS gateway, but got into a processing queue.

If a message "Sorry, due to an internal error the service is temporarily unavailable..." is displayed after registration on the portal, an error has occurred while transmitting a message to an SMS gateway which is probably unavailable at the moment. Request a password after some minutes. If the error occurs again,

check SMS gateway availability from the server eltex-notification-gw. If the gateway is pinged, write eltex-notification-gw logs when sending an SMS and mail them to Eltex.

**- After performing user authorization and clicking 'Continue', redirection to a website specified in the portal configuration does not work.**

If there is no Internet access, the problem relates to configuration of redirection and white lists in a tariff. If a tariff with white lists is configured correctly, check if addresses of DNS servers are specified on access points and available from them.
If Internet access is provided, a wrong redirection address is specified in virtual portal configuration. Check virtual portal and tariff settings according to the instruction: SoftWLC. Setting tariffs for portal authorization

**3. wpa-personal**

The points to be checked are listed below.

**- A level of a signal from a client's device on an access point.**
If a signal level is -75 dB or lower, a client should get closer to an access point for this AP to "see" a client with signal level -65dB.

**- Correctness of an authorization key specified by a user.**

**- If authorization has been successful, check if a client device receives an IP address.**
If an address on a device is specified manually, enable dynamic address obtaining.
If a device does not receive an address from a DHCP server, perform diagnostics of a DHCP server and network.

**- If a device has an IP address, ping a default gateway and DNS servers.**

**4. wpa-personal + portal authorization**

The points to be checked are listed below.

**- A level of a signal from a client's device on an access point.**
If a signal level is -75 dB or lower, a client should get closer to an access point for this AP to "see" a client with a signal level -65dB.

**- Correctness of an authorization key specified by a user.**

**- If authorization has been successful, check if a client device receives an IP address.**
If an address on a device is specified manually, enable dynamic address obtaining.
If a device does not receive an address from a DHCP server, perform diagnostics of a DHCP server and network.

If a device has an IP address, but authorization process has not been completed, a gateway will not be pinged.

**- Check if redirection works correctly. Open your browser and try to access a website via http (not https!), for example** http://www.sberbank.ru**/,** http://www.rostelecom.ru/**,** http://eltex.nsk.ru/**.**
If redirection does not work, perform diagnostics. The instruction SoftWLC. Setting tariffs for portal authorization may help you.

**- Redirection has worked, a user has been authorized but has not received an SMS with a password.**
If after registration on the portal a message "*Data is being processed. Wait for an SMS to the entered number '79xxxxxxxxx'*" is displayed, but waiting time is beyond 5 minutes, a message has been delivered to an SMS gateway, but got into a processing queue.
If a message "*Sorry, due to an internal error the service is temporarily unavailable...*" is displayed after registration on the portal, an error has occurred while transmitting a message to an SMS gateway which is probably unavailable at the moment. Request a password after some minutes. If the error occurs again, check SMS gateway availability from the server eltex-notification-gw. If a gateway is pinged, write eltex-notification-gw logs when sending an SMS and mail them to Eltex.

**- After user authorization and clicking "Continue", the redirect to a website specified in the portal configuration does not work.**
If there is no Internet access, the problem relates to configuration of redirection and white lists in a tariff. If a tariff with white lists is configured correctly, check if addresses of DNS servers are specified on access points and available from them.

If Internet access is provided, but redirection does not work, a wrong redirection address is specified in virtual portal configuration.
Check virtual portal and tariff settings according to the instruction: SoftWLC. Setting tariffs for portal authorization

**5. wpa-enterprise**

The points to be checked are listed below.

**- A level of a signal from a client's device on an access point.**
If a signal level is -75 dB or lower, a client should get closer to an access point for this AP to "see" a client with a signal level -65dB.

**- Correctness of RADIUS connection settings specified in SSID configuration: IP address, secret key.**

**- Correctness of data specified by a user during authorization.**

In adddition, check if a user account domain is the same as a SSID domain on which a user is authorized. Check if there are any limitations on the number of connections in account settings, or time (traffic) limits on exceeding of which an entry is blocked. Check if an account lifetime had expired.

**- Is a RADIUS certificate accepted by a user as a trusted one?**
If it is not, delete a network on a client's device and reestablish a connection. A user will be invited to accept a certificate again.

**If after performing these steps the problem has not been solved, please, contact our tech support and describe your problem and actions taken to address it.**

# v1.14_Troubleshooting of obtaining IP addresses by Wi-Fi users

## Initial diagnostics

1. A DHCP server is started.
2. Make sure that VLAN ID specified in SSID configuration is correct.
3. Make sure that a user connects to an appropriate SSID on the AP under consideration.
4. If encryption is implied for a SSID, make sure that a user has passed authorization successfully.
5. Check if an address is received by another SSID of the same access point (AP).
6. Check if an address is received by another device (smartphone/laptop).
7. Select the mode "Get an address via DHCP" in network settings of a user's device.
8. Specify a static IP address on a client, check if a gateway is accessible using ping (icmp).

If these settings are correct, move to checking configuration of the server and networking functions. To run diagnostics, it is necessary to know a MAC address of a client's device and have an opportunity to initiate providing a client with an address via DHCP.

## Checking a DHCP server

To check DHCP server operation, analyse its logs.
The three main problems can be seen from logs:

- Discover is absent.
- Discover is present, Offer is absent.
- Discover and offer are present, Request is absent.

**1. Discover from a client's device is absent in logs.**

Start tcpdump on an interface of a server to which Discover was supposed to get. Check the server for Discover.

- If Discover is absent in a dump, check network settings, a DHCP-relay and its connections.
- If Discover is present in a dump, but absent in logs, check the server configuration (paragraph 1.1).

1.1. Discover is present in a dump, but absent in logs.

Discover is ignored because it arrives on an interface that is not listened by the server. Determine the interface that Discover gets on and add this interface to DHCP server configuration.

In the file **/etc/default/isc-dhcp-server** all listened interfaces should be listed, for example:
`INTERFACES="eth0 eth1"`

**2. Discover is present in DHCP server logs, but Offer is absent.**

To determine the cause, check DHCP server logs. Common causes:

- one of the subnetworks used is not specified
- classes are specified incorrectly
- pool vacant addresses exhaustion
- failover problems

### 2.1 One of the subnetworks used is not specified

Subnetworks containing addresses of listened interfaces and a DHCP-relay (if used) should be specified in the file **/etc/dhcp/dhcpd.conf**. Even if addresses from these subnetworks are not allocated by the server, for example:

```
subnet 192.168.1.0 netmask 255.255.255.0 {}
```

### 2.2 Pool vacant addresses exhaustion

One of the common causes is a case when a server runs out of vacant addresses. To check it, use a guide: ISC DHCP server pool range usage monitoring

**3 Discover and Offer are present in DHCP server logs, but Request is not.**

Use tcpdump for the interface that Discover arrives on and check this dump for Offer.

- If Offer is absent in a dump, a wrong route to a user subnetwork is specified on a server. Hence, Discover is sent to one interface, but Offer is sent to another one and does not reach a recipient. Check and reconfigure routing on the server.
- If Offer is present in the dump, check a DHCP relay and a connection between DHCP server and DHCP relay.

**4 Checking a connection between a DHCP server and a DHCP relay**

Ping a DHCP relay from a server. Ping should be done from an appropriate interface.

## Checking a DHCP relay

### Debugging in the Scheme with GRE

1. Checking GRE tunnels status.

To check status of GRE tunnels,

- Identify "primary" IP address of an AP via EMS management system. A primary address is specified in the tab "Access" of the main window and in the section "EMS Monitoring".
- On ESR, check a list of the AP's GRE tunnels. Use the following command:

```
show tunnels status | include <XXX.XXX.XXX.XXX>
```
where **XXX.XXX.XXX.XXX** – AP primary IP

The command will return a list of tunnels built by this AP.

- If there are no tunnels, check DHCP server configuration and IP connectivity between an AP and ESR.
- If there is one tunnel, check DHCP server configuration and ESR configuration.
- If there are two tunnels, check if sub-tunnels with VLANs consistent with AP configuration are established for the second tunnel.

2. Creating a traffic dump on a SUB-GRE tunnel of an AP under consideration.

To get a dump, connect under the 'techsupport' user, enable 'su' mode and enter the command:

```
tcpdump –i dygreXXX.YYY –evn –c100
```

where **XXX** is a GRE tunnel number found on the previous step, **YYY** isVLAN ID

In a dump received, perform a search for Discover from a client:

- If there is no Discover in a dump, an AP has not probably been able to establish a tunnel correctly. Check DHCP server configuration (option 43, suboption 12) and AP configuration.
- If Discover is present in the dump, but Offer is absent - move on to checking exchange with a DHCP server (paragraph 3).

3. Creating a traffic dump when exchanging packets with a DHCP server.

To get a dump, connect under the 'techsupport' user, enable 'su' mode and enter the command:

```
tcpdump –i te1_YYY.ZZZ –evn –c100
```
, where **YYY**– ESR port number, **ZZZ** – VLAN number.

- If there is no Discover in the dump, something is wrong with ESR configuration.
- If Discover is transmitted to a DHCP server, but Offer is absent – there is a problem with connection between a DHCP server and ESR.
- If Discover and Offer are present, but Request does not participate in exchange, there is a problem with ESR configuration.

### Debug in the Scheme without GRE

1. Creating a traffic dump on an interface directed to a client.

Find Discover from a client during the dump analysis.

- If there is no Discover, check:

1. Firewall configuration on a DHCP-relay.
2. Network configuration for connection with an AP.
3. AP configuration.

- If Discover is present, but Offer is absent – move on to checking DHCP server exchange.

2. Creating a tcpdump of DHCP server exchange.

- If there is no Discover in a dump – there is a problem with DHCP relay configuration. Check a firewall and routing configuration on a DHCP relay.
- If Discover is transmitted to a DHCP server, but Offer is absent – there is a problem with connection between a DHCP server and a DHCP relay.
- If Discover and Offer are present, but Request does not participate in exchange – there is a problem with firewall settings on a DHCP-relay.

## Checking an access point

Configure an opened SSID without authorization in the same VLAN with the SSID considered. According to an instruction on creating a dump (pcap) of an access point, create dumps on a radio interface to which a user is connected and on eth interface. Results should be interpreted depending on a connection scheme used.

**For any scheme:**

- If Discover from a user is absent in a dump with a radio interface, there is a problem with a client's device. Probably it has not connected to the network or does not require an address for some reasons.

**For the scheme with GRE:**

- If Discover from a user is present on a radio interface but absent on eth, a GRE tunnel for user traffic has not been built because an access point received an incorrect suboption 12 when getting a primary address. Check DHCP server configuration (option 43, suboption 12).
- If Discover is present in both dumps, packets are transmitted from an AP. Make sure that ESR receives packets.

**For the scheme without GRE:**

- If Discover is present in dumps from the radio interface and eth, but absent on a DHCP-relay, a user VLAN is not either configured on the end device or forwarded to the DHCP-relay.

## v1.14_Network diagnostics on ESR

Diagnostics on ESR needed to define if the network operation is correct.

### Check for the core availability from access point management networks

Command:

```
ping <server ip address> source ip <bridge ip address>
```

Example:

```
ESR100# ping 192.168.1.1 source ip 192.168.2.2
PING 192.168.1.1 (192.168.1.1) from 192.168.200.4 : 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.128 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.116 ms
^C---
192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.116/0.122/0.128/0.006 ms
ESR1000#
```

**192.168.1.1** – EMS server addresswhere:

**192.168.2.2** – the address of the ESR bridge that is the access point management network's gateway

### Check for tunnels

Management tunnel check command:

```
show tunnel status | include "<tunnel terminating ip address>"
```

Example:

```
ESR1000# show tunnel status | include "10.203.5.11"
softgre 10         Up      Up      1462     10.203.5.11        10.203.37.235      61 days, 2
 hours, 16
softgre 23         Up      Up      1462     10.203.5.11        10.203.36.59       6 days, 2
 hours, 46
softgre 27         Up      Up      1462     10.203.5.11        10.203.40.114      34 days, 2
 hours, 38
softgre 28         Up      Up      1462     10.203.5.11        10.203.37.124      34 days, 17
 hours, 56
softgre 29         Up      Up      1462     10.203.5.11        10.203.40.80       34 days, 2
 hours, 38
```

where **10.203.5.11** – the address of the interface where management tunnels terminate

## Interface traffic check

Command:

```
show interfaces utilization
```

Example:

```
ESR1000# show interfaces utilization
Interface       Period, s     Sent,          Recv,          Frames Sent   Frames Recv
                              Kbit/s         Kbit/s
-------------   -----------   -----------    -----------    -----------   -----------
gi1/0/1         5             80             49466          37            5960
gi1/0/2         5             76873          27311          11301         5413
gi1/0/3         5             0              0              0             0
...

gi1/0/24        5             0              0              0             0
te1/0/1         5             0              0              0             0
te1/0/2         5             0              0              0             0
po1             5             76954          76778          11339         11373
bridge 2        5             172            115            99            101
bridge 3        5             90             136            53            57
bridge 4        5             49182          24367          5995          5301
bridge 5        5             24920          48515          5261          5976
bridge 6        5             51703          26331          6136          5430
bridge 7        5             0              0              0             0
bridge 8        5             273            12             29            13
bridge 9        5             14             274            12            31
bridge 10       5             0              0              0             2
```

⚠ Null values in 'Sent' or 'Recv' columns demonstrate the lack of activity on the relevant bridge. If the bridge is intended for users, failures are possible.

## Check for the DHCP availability from user network

Command:

```
ping <server ip address> source ip <bridge ip address>
```

Example:

```
ESR1000# ping 192.168.1.2 source ip 100.65.64.4
PING 192.168.1.2 (192.168.1.2) from 100.65.64.4 : 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.176 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.152 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.312 ms
^C
--- 192.168.114.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.152/0.213/0.312/0.071 ms
ESR1000#
```

**192.168.1.2** – DHCP server's addresswhere:

**100.65.64.4** - the address of the ESR bridge that is the user network's gateway

## Check for external resources availability from a user network bridge

Command:

```
ping <server ip address> source ip <bridge ip address>
```

Example:

```
ESR1000# ping 8.8.8.8 source ip 100.65.64.4
PING 8.8.8.8 (8.8.8.8) from 100.65.24.1 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=16.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=15.8 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 15.892/15.998/16.105/0.165 ms
ESR1000#
```

**8.8.8.8** – any external resource that should be available for a userwhere:

**100.65.64.4** - the address of the ESR bridge that is the user network's gateway

## v1.14_ISC DHCP server pool range usage monitoring

ISC DHCP server implementation has no effective methods for pool range usage monitoring.

There might be situations where the server has covered the entire possible range and ignores new devices' requests. In this case,a message (of messages) of the following type can be found in the log:

```
Feb 10 01:01:01 EltexDHCP dhcpd: DHCPDISCOVER from aa:bb:cc:dd:ff:00 via
100.10.1.1: peer holds all free leases
```

In order to count pool usage ratio and prevent such situations, **dhcpd-pools** utility program can be used. The utility build for ubuntu14 x64 is attached.
dhcpd-pools_2.28-1-trusty_amd64.deb

To install the program using release package, copy it to a SoftWLC server and unpack by entering:

```
sudo dpkg -i dhcpd-pools_2.28-1-trusty_amd64.deb
```

After that, run the utility with:

```
sudo dhcpd-pools -c /etc/dhcp/dhcpd.conf -l /var/lib/dhcp/dhcpd.leases -o ./
sampleoutput.txt
```

where
**/etc/dhcp/dhcpd.con** — main DHCP server configuration file location,
**/var/lib/dhcp/dhcpd.leases** — lease file path,
**./sampleoutput.txt** — a result output file.

Project sample:

```
cat sampleoutput.txt
Ranges:
shared net name     first ip           last ip            max   cur    percent  touch   t+c  t+c
perc
All networks        122.0.0.10       - 122.0.0.200        191     7      3.665     47    54
28.272
All networks        123.0.0.10       - 123.0.0.200        191     2      1.047      9    11
5.759
All networks        124.0.0.10       - 124.0.0.200        191     2      1.047     57    59
30.890
All networks        200.0.0.10       - 200.0.0.30          21     0      0.000      0     0
0.000

Shared networks:
name                   max   cur     percent  touch    t+c  t+c perc

Sum of all ranges:
name                   max   cur     percent  touch    t+c  t+c perc
All networks           594    11      1.852     113    124    20.875
```

Results may include:
**shared net name** — the network DHCP server leases addresses from,
**first ip, last ip** — the first and the last addresses in the pool,
**max** — the pool range,
**cur** — the number of issued IP addresses with an active lease (addresses used to date),
**percent** — cur/max ratio expressed as a percentage,
**touch** — the number of issued IP addresses with a lease expired,
**t+c** — the total number of issued IP addresses;
**t+c perc** — t+c/max ratio, expressed as a percentage.

The utility has other opportunities as well, further information can be found on its developer's website http://dhcpd-pools.sourceforge.net/ or in the manual.

## v1.14_tomcat service monitoring on the SoftWLC server

To monitor tomcat service, a special "tomcat7-admin" package is used. It can be downloaded from Ubuntu repositories:

```
apt-get install tomcat7-admin
```

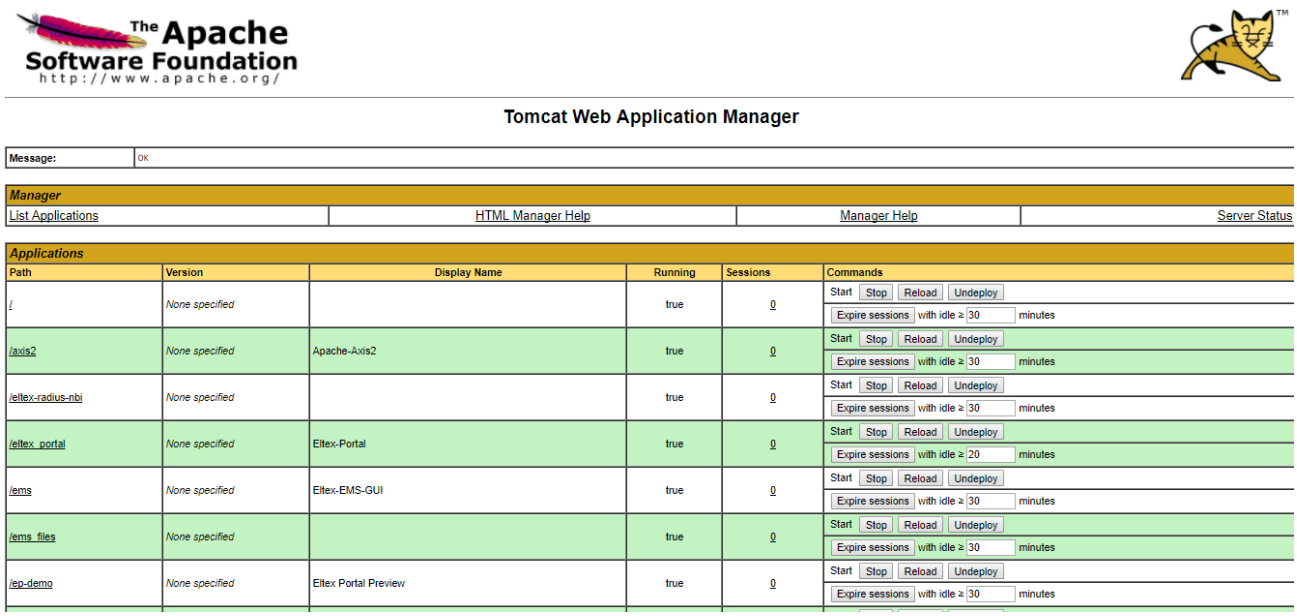
When the package is installed, user account should be set up for authorization in the monitoring system: The file $TOMCAT_HOME/conf/tomcat-users.xml (standard SoftWLC installation uses /var/lib/tomcat7/conf/tomcat-users.xml path) should be supplemented by the following lines:

```
<role rolename="manager-gui"/>
<user username="admin" password="admin" roles="manager-gui"/>
```

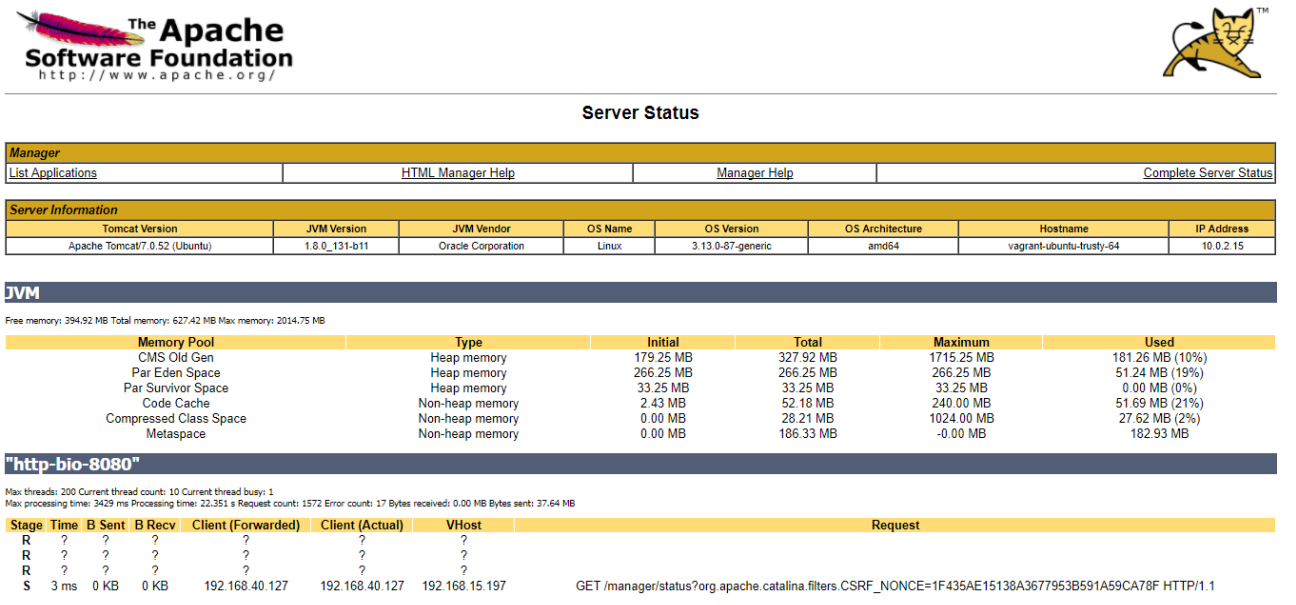
After that, restart tomcat7 service:

```
service tomcat7 restart
```

To use service monitoring GUI, enter the following URL in your browser: http://localhost:8080/manager, where localhost should be replaced by the server's IP address.
Login = **admin**, password = **admin**, according to the tomcat-users.xml configuration file.
GUI for monitoring is as follows:




Applications monitoring




Resources monitoring

Further guidance can be found here: http://tomcat.apache.org/tomcat-7.0-doc/manager-howto

## v1.14_RADIUS debug obtaining

Eltex-radius package has been supplemented by 1.7-28-build eraddebug and eradmin utilities (raddebug and radmin in the original) from Freeradius parent package.
eraddebug allows obtaining debugging output (like the output when using radiusd -X) from a running server. Therefore, it is possible to obtain debugging information without impacting service availability in Production.
For RADIUS server proper operation the following settings are required:

**/etc/eltex-radius/servers/control**

```
listen {
        type = control
        socket = ${run_dir}/${name}.sock
        uid = eltxrad
        gid = eltxrad
        mode = rw
}
```

the settings above are stored in the file `/etc/eltex-radius/servers/control` of eltex-radius package.

To start the server, the following commands are used:

```
sudo -u eltxrad eradmin
sudo -u eltxrad eraddebug
```

The first command launches eradmin utility, and the second command runs eraddebug script under eltxrad username. To obtain debugging output, the second command is used. eradmin is an independent utility for RADIUS server administration. eraddebug is a shell script wrapper around eradmin that automates the server debugging process.

**Attention!** Set conditions to prevent information overflow.

### Options

| Option | Description |
|---|---|
| -c condition | Set a specific debug condition. The format of conditions is specified on: http://freeradius.org/radiusd/man/unlang.html#lbAF |
| -f socket_file | The path to the control socket that is defined with `socket = ${run_dir}/${name}.sock`. Usually reads configuration files. If something goes wrong, set a socket manually. |

| Option | Description |
|---|---|
| -i ipv4-address | Show debug output for an access point having IPv4 address. The equivalent command using conditions: -c '(Packet-Src-IP-Address == ipv4-address)' |
| -d config directory | The RADIUS configuration directory, usually `/etc/eltex-radius`. |
| -n mname | Read raddb/name.conf instead of raddb/radiusd.conf. |
| -I ipv6-address | Show debug output for an access point having IPv6 address. This option is equivalent to using: -c '(Packet-Src-IPv6-Address == ipv6-address)' |
| -t timeout | Debug output printing timeout in seconds. Stop printing debug output after "timeout" seconds. The default timeout is 60 seconds. Use "-t 0" to disable the option. |
| -u name | Show debug output for a certain user. This option is equivalent to using: -c '(User-Name == name)' |

-t option should be used with extreme caution! Using "-t 0" in Production is not recommended.

**Examples**

```
eltex@ubuntu:/$ sudo -u eltxrad eraddebug -u wifiuser
```

This command run not under the root superuser, executes eraddebug script under the eltxrad name, shows debugging output for the wifitester user and stops automatically after 60 seconds (default timeout).

```
eltex@ubuntu:/$ sudo -u eltxrad eraddebug -t 300 -u wifiuser
```

This command run not under the root superuser, executes eraddebug script under the eltxrad name, shows debugging output for the wifitester user and stops automatically after 5 minutes.

```
root@ubuntu:/# eraddebug -t 0 -u wifiuser
```

When running under the root superuser, sudo is not required. This command will show debug output until it is stopped manually with Ctrl+C.
Sources:

- Official 'man' http://freeradius.org/radiusd/man/raddebug.html
- The description of the unlang processing 'un-language' used for configuration http://freeradius.org/radiusd/man/unlang.html

## v1.14_Eltex-portal error codes table

**Error codes table:**

| Code | Description | Mnemonics | Error cause. Possible solution. |
|---|---|---|---|
| 403 | Access is forbidden | FORBIDDEN | |
| 404 | The source is not found | NOT_FOUND | Check the accessibility of the server for the access point, tomcat servers operation and eltex-portal. Make sure that the portal's URL<br>defined in SSID/VAP settings is correct. |
| 500 | Internal error | INTERNAL_SERVER_ERROR | Server error. Check logs for errors. |
| 1001 | Access point's header is missing | AP_HEADER_MISSING | HTTP header is missing, access point version 1.9 or lower is probably used. |
| 1002 | Access point's secret key is incorrect | AP_INCORRECT_SECRET | Verify that radius keys for an access point and a server are correct. |
| 1101 | BRAS is disabled | BRAS_DISABLED | Check if BRAS accessb is enabled in the Portal Constructor. |
| 1102 | Request BRAS parameter is missing. | BRAS_PARAM_MISSING | Check the 1101 error code and ESR BRAS license. |
| 1103 | BRAS session disconnect | BRAS_DISCONNECT_FAILED | Disconnect with an unknown session was sent to BRAS. |
| 1104 | BRAS redirection error | BRAS_ACCEPT_ERROR | Check subscriber-control settings on an ESR with BRAS. |
| 1105 | BRAS reject error | BRAS_REJECT_ERROR | BRAS rejected the request. |
| 1201 | The portal is not found | PORTAL_NOT_FOUND | Check if the Virtual portal name field in SSID/WAP settings contains an existing portal's name. |
| 1202 | The portal is not initialized | PORTAL_NOT_INIT | Check if the eltex-portal service operates correctly, restart it. Make sure that the portal specified in SSID/VAP settings is created and available in the Portal Conctructor. |
| 1301 | No tariffs are available for a user | NO_AVAILABLE_TARIFFS | Set tariffs plan in the "Tariffs plan" tab of the Portal Constructor. Make sure that tariffs are set on the selected portal. |
| 1401 | A language is not selected | LANGUAGE_NOT_SELECTED | Check if a language is selected in the "Language settings" tab of the Portal Constructor. |
| 1501 | Advertising platform integration is disabled | ADVERT_DISABLED | Check if advertising integration is enabled in the "Advertising platform" tab of the Portal Constructor. |

| Code | Description | Mnemonics | Error cause. Possible solution. |
|---|---|---|---|
| 1502 | Advertising platform handler is missing. | ADVERT_HANDLER_MISSING | Check if some advertising platform is selected in the "Advertising platforms" tab of the Portal Constructor. Check if configuration is correct (address availability for the server, client ID). |
| 1601 | NGW is not available | NGW_NOT_AVAILABLE | Check if the eltex-ngs server is configured correctly. Make sure that the parameters in the "NGW access" tab of the Portal Constructor are correct. |
| 1701 | No authentication methods are available | NO_AUTH_METHODS_AVAILABLE | Make sure that authentication mode (ESIA, mode, confirmation methods) is selected in "Common settings" tab of the Portal Constructor. |
| 1801 | ESIA signature error | ESIA_SIGNATURE_ERROR | Check if ESIA Login settings in the Portal Constructor are correct. |
| 1802 | ESIA request error | ESIA_REQUEST_FAILED | Check if the ESIA system is available and configured correctly. |
| 1901 | SSID check error | SSID_CHECK_FAILED | Check if SSID is configured correctly on the access point. |
| 2001 | Registration error | REGISTRATION_ERROR | Check registration credentials. |
| 2002 | Authentication error | AUTHENTICATION_ERROR | Check auth data. |
| 2101 | L2 subnet is not found | L2_SUBNET_NOT_FOUND | Make sure that L2 subnet settings for BRAS in PCRF tab are correct. |

Service operation log is written to the file **/var/log/eltex-portal/log_ep.txt**

# v1.14_SoftWLC modules (EN)

## v1.14_APB (EN)


- Description
- Service management
- Configuration
  - /etc/default/eltex-apb
  - /etc/eltex-apb/apb.properties
  - /etc/eltex-apb/ehcache.xml
  - /etc/eltex-apb/hosts.json
- Configuring access points connection to APB


### Description

The module Eltex-APB is implied to support information exchange between access points. Provides:

- Roaming of users connected via the WEB portal authorization authorization.
- Configuration and transmission of public address lists during portal authorization,

The service is installed using the package **eltex-apb**.

### Service management

| Operation | Command | Response |
|---|---|---|
| Status check | `service eltex-apb status` | The service is running<br>`eltex-apb is running with pid <pid>`<br><br>The service is not running<br>`eltex-apb is not running` |

| Operation | Command | Response |
|---|---|---|
| Service start | `service eltex-apb start` | The service has been started<br>`Starting eltex-apb ... eltex-apb started`<br><br>The service is already running<br>`eltex-apb is already running` |
| Service stop | `service eltex-apb stop` | The service has been successfully stopped<br>`Stopping eltex-apb ... eltex-apb stopped`<br><br>The service has not been stopped, as it was not started<br>`eltex-apb is not running rm: cannot remove '/var/run/eltex-apb.pid': No such file or directory` |
| Service restart | `service eltex-apb restart` | The service has been successfully restarted<br>`Stopping eltex-apb ... eltex-apb stopped Starting eltex-apb ... eltex-apb started` |

## Configuration

### /etc/default/eltex-apb

- contains the main service settings:

- A listened port:

```
PORT=8090
```

- Request queue length. When a queue is full, new requests will be ignored by a server, until old requests are processed (by default, request will not be queued):

```
ACCEPT_QUEUE_SIZE=0
```

- Maximum message buffer size, in bytes:

```
MAX_TEXT_MESSAGE_BUFFER_SIZE=262144
```

- Memory allocated for service operation (memory is allocated for a process, not for a cache specified in **/etc/eltex-apb/ehcache.xml**):

```
JAVA_INIT_HEAP=128m
JAVA_MAX_HEAP=2048m
```

### /etc/eltex-apb/apb.properties

- the file contains settings for connection to the Mercury service,

```
mercury.host=localhost
mercury.port=6565
mercury.pool.size=100
```

required files' locations

```
# Config filePath to cache
cache.config=/etc/eltex-apb/ehcache.xml

# list of permitted files to
hosts.file=/etc/eltex-apb/hosts.json
```

and subscription request waiting time after an access point's connection to a server (in seconds)

```
subscribe.idle.timeout=60
```

Maximum number of outgoing messages in a queue for each session

```
session.outgoingQueue=100
```

### /etc/eltex-apb/ehcache.xml

- system settings for storing data on Wi-Fi users connected to a portal. If necessary, the file's name and location can be changed in **/etc/eltex-apb/apb.properties**.

- Amount of RAM allocated for a table of authorized users is configured in:

```
<cache name="users"
       maxBytesLocalHeap="200M"
       eternal="false"
       timeToLiveSeconds="43200"
       memoryStoreEvictionPolicy="LRU">
```

parameter
maxBytesLocalHeap="200M"

- Amount of RAM allocated for a table with public address lists is configured in:

```
<cache name="hosts" maxBytesLocalHeap="128M" eternal="true">
    <persistence strategy="none"/>
</cache>
```

parameter
maxBytesLocalHeap="200M"

### /etc/eltex-apb/hosts.json

- the file in json format that contains a set of public address lists. Lists of IP addresses permitted for access before portal authorization are configured in this file. If necessary, the file's name and location can be changed in **/etc/eltex-apb/apb.properties**.

Listing of hosts.json:

```
[
  {
    "mobility-domain-list": [
      {
        "mobility-domain": "nsk.ru",
        "radius-domain": "root",
        "ssid": "Eltex-Local"
      }
    ],
    "permitted-ip-list": [
      "eltex.nsk.ru",
      "eltex.org"
    ]
  },
  {
    "mobility-domain-list": [
      {
        "mobility-domain": "spb.ru"
      },
      {
        "mobility-domain": "msk.ru",
        "radius-domain": "root"
      }
    ],
    "permitted-ip-list": [
      "rostelecom.ru"
    ]
  },
  {
    "permitted-ip-list": [
      "213.222.201.16",
      "213.222.198.16",
      "213.180.193.51",
      "192.225.158.3",
      "180.97.33.83",
      "178.162.216.178" ........
    ]
  }
]
```

By default, some permitted IP addresses are specified in this configuration file. The list is applied for all users.
If required, the list can be expanded as in the following examples:

- White list (a list of IP addresses that a client can access before authorization), common to all connected access points is specified in the following format:

```
[{
  "permitted-ip-list": [
      "esia-portal1.test.gosuslugi.ru",
      "esia.gosuslugi.ru",
  ]
}]
```

- To assign a white list to access points with a certain SSID and domain, the following format is used:

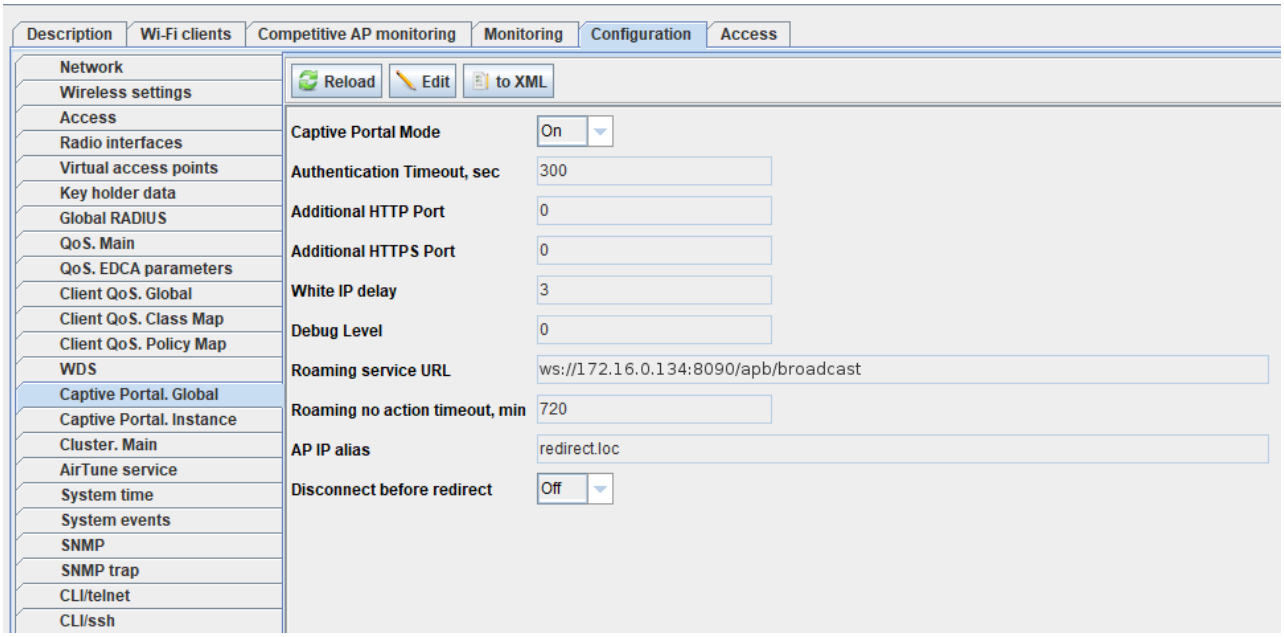
```
[{
  "mobility-domain-list": [
    {
      "mobility-domain": "nsk.ru",
      "radius-domain": "root",
      "ssid": "Eltex-Local"
    }
  ],
  "permitted-ip-list": [
    "eltex.nsk.ru",
    "eltex.org"
  ]
}]
```

That means if information on a user whose mobility domain is nsk.ru, radius-domain is root, and SSID is Eltex-Local gets on the server, the addresses eltex.nsk.ru and eltex.org will be added to default ones specified in the list of IP addresses that the user is permitted to access without portal authorization. That is, addresses included into the "permitted-ip-list" will be applied to a user if all keys specified within one "mobility-domain list" fully match.
If user parameters meet the criteria of several rules, this user will be permitted to access IP addresses from all these rules.

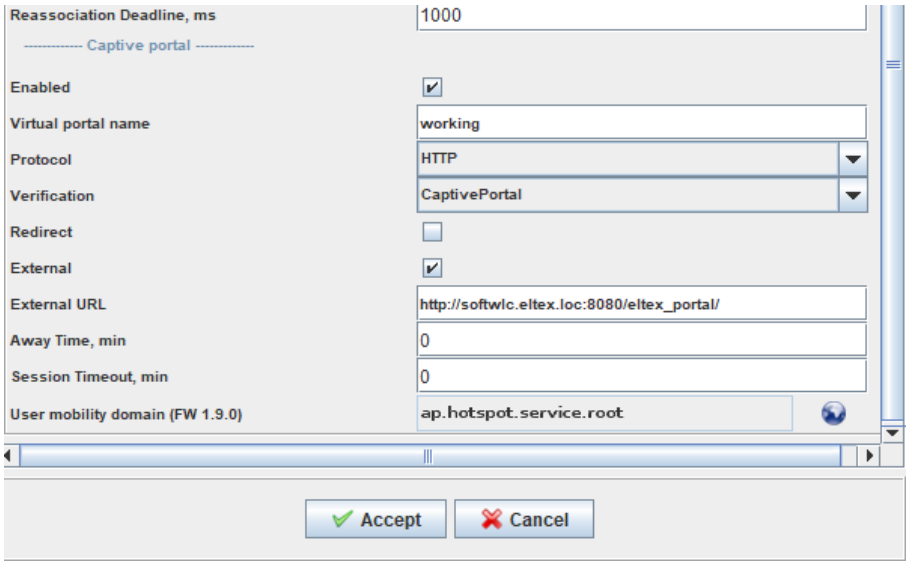
> ⚠ The parameter **ap-location** is now used instead of **mobility-domain**. It is fully consistent with it, but is located in the Network settings section.

## Configuring access points connection to APB

Connection to the APB service on an access point can be configured via GUI EMS.
To configure user roaming during portal authorization, open the section **Configuration → Captive Portal.Global** and specify the address **Roaming Service URL =** ws://<APB IP address>:8090/apb/broadcast




where **<APB IP address>** is the address of APB accessible from the AP management network. Configure *«Roaming no action timeout»* (after which an AP will delete old/inactive entries about roaming clients). The value of *«Roaming no action timeout»* should be higher than a maximum lifetime of a tariff After that, open a configured SSID in the tab *"Virtual access points"* and specify a *«User Mobility Domain»* in Captive Portal settings (the domain should be the same for all access points that will operate in a roaming).




## v1.14_Auth Service (EN)


- Description
  - Working with MySQL remote database
- Service management

- Configuration
  - /etc/eltex-auth-service/sql.conf
  - server = "localhost"
  - #port = 3306
  - login = "eltexauthservice"
  - password = "eltexauthpassword"
  - The table is stored in eltex_auth_service database. It contains the addresses of clients that have rights to send user authorization requests. If a client is not included into the table, authorization requests will be ignored. When the contents of the table is changed, restart eltex-auth-serviceNAS table

## Description

The service is used for Admin Panel, Portal Constructor and NBI users authorization.
Use **eltex-auth-service** package for installation.

The package requires **eltex-radius** package pre-installed.

**Working with MySQL remote database**
If **eltex-auth-service** is configured to work with **Mysql** remote server, it is necessary to change the order of package downloading for service autostart:

```
echo "start on runlevel [2345]" > /etc/init/eltex-radius.override
echo "start on runlevel [2345]" > /etc/init/eltex-auth-service.override
```

## Service management

| Operation | Command | Response |
|---|---|---|

| | | |
|---|---|---|
| Status check | `service eltex-auth-service status` | Service is running<br>`eltex-auth-service start/ running, process <pid>`<br><br>Service is waiting<br>`eltex-auth-service stop/ waiting` |
| Service start | `service eltex-pcrf start` | Service has been started<br>`eltex-auth-service start/ running, process <pid>` |
| Service stop | `service eltex-auth-service stop` | Service has been stopped successfully<br>`eltex-auth-service stop/ waiting` |
| Service restart | `service eltex-auth-service restart` | Service has been restarted successfully<br>`eltex-auth-service stop/ waiting`<br>`eltex-auth-service start/ running, process 16737` |

## Configuration

### /etc/eltex-auth-service/sql.conf

The file contains the parameters for the service to access **eltex_auth_service** database.

```
server = "localhost"

#port = 3306

login = "eltexauthservice"

password = "eltexauthpassword"
```

The table is stored in **eltex_auth_service** database. It contains the addresses of clients that have rights to send user authorization requests. If a client is not included into the table, authorization requests will be ignored. When the contents of the table is changed, restart **eltex-auth-service**NAS table

## v1.14_Eltex Portal (EN)


- Description
- Service management
- Configuration
    - /etc/eltex-portal/application.conf
    - /etc/default/eltex-portal
    - /etc/eltex-portal/log4j2.xml
- Log errors description


### Description

WEB portal is included into SoftWLC project to implement Hotspot clients authorization model. An unknown user can connect to an access point without getting login and password in advance. But if he (or she) tries to access the Internet via a browser, he will be redirected to a WEB portal page where authorization or credentials obtaining (for example, via SMS) can be performed. During authorization, a user can see advertisement banners customized in accordance with operator's requirements.

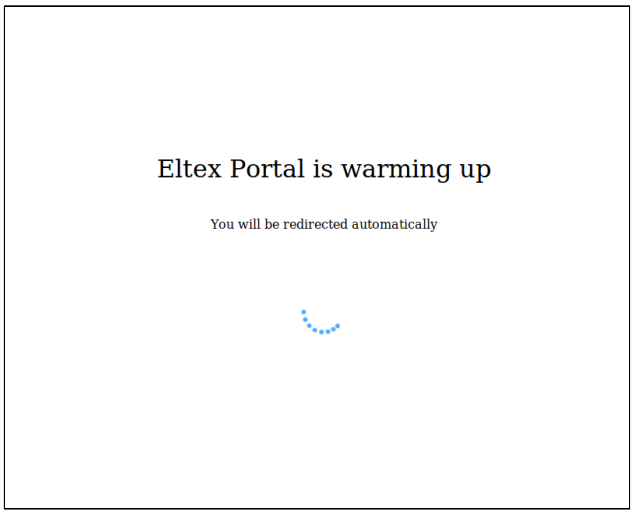
The service is used for displaying virtual portals' pages and for registration and authorization of Wi-Fi users connected via Eltex access points or ESR/BRAS.

Installation is performed using **eltex-portal** package.

"Warming up" page will be dispayed instead of the portal during eltex-portal service initialization until the service is fully loaded. It shows that both portal initialization and service module configuration

processes have not been finished yet. After eltex-portal service is fully loaded, the user will be redirected to the main page of the portal.

An example of a portal initialization page:




## Service management

| Operation | Command | Response |
|---|---|---|
| Status check | `service eltex-portal status` | Service is running<br>`eltex-portal start/running, process <pid>`<br><br>Service is waiting<br>`eltex-portal stop/waiting` |
| Service start | `service eltex-portal start` | Service has been started<br>`eltex-portal start/running, process <pid>`<br><br>The service is already running<br>`start: Job is already running: eltex-portal` |

| | | |
|---|---|---|
| Service stop | `service eltex-portal stop` | Service has been stopped successfully<br>`eltex-portal stop/waiting`<br><br>Service has not been stopped, as it was not started<br>`stop: Unknown instance:` |
| Service restart | `service eltex-portal restart` | Service has been restarted successfully<br>`eltex-portal stop/waiting`<br>`eltex-portal start/running, process <pid>`<br>`eltex-portal start/running, process <pid>`<br>`stop: Unknown instance:` |

## Configuration

### /etc/eltex-portal/application.conf

main configuration file. Default configuration example:

```
portal {
    defaultRedirectUrl = "http://eltex-co.ru"
    tariffCheckerPeriod = 1440
}

jetty {
    https {
        port = 9443
        keystorePass = 12345
        keystoreFile = /etc/eltex-portal/localhost.pfx
        keystoreType = PKCS12
        keyAlias = 1
        ciphers = [
            TLS_RSA_WITH_AES_128_CBC_SHA256
            TLS_RSA_WITH_AES_128_CBC_SHA
            TLS_RSA_WITH_AES_256_CBC_SHA256
            TLS_RSA_WITH_AES_256_CBC_SHA
        ]
    }

    accessLog {
        enabled = true
        directory = /var/log/eltex-portal/

        # <default> : NCSA format
        # <custom>  : customized NCSA with additional parameters
        format = default
        retainDays = 30
        append = false
        logCookies = true
        logAP = true
        logBRAS = true
    }
}

database {
    host = localhost
    port = 3306
    name = ELTEX_PORTAL
    user = javauser
    password = javapassword

    readOnly = true

    pool {
        # Time to wait for a connection
        connectionTimeout = 10s
        # Time to wait for connection validation
        validationTimeout = 3s
```

```
        min = 1
        max = 10
    }

    cache {
        # Limit of cached simple entries count (for each query type)
        maxEntries = 1000
        # Limit of total cached portal resources size
        maxResourceBytes = 32m
        # Maximum time to retain items in the cache
        expireTime = 2m
    }
}
```

| Parameter | Description |
|---|---|
| **portal** | |
| **defaultRedirectUrl** | The address where the user will be redirected if his session should be restarted. It should be set in accordance with http protocol. |
| **tariffCheckerPeriod** | The interval for checking tariff availability on portals. If there are no available tariffs, the error message is generated. |
| **jetty** | |
| **https** | Configuring container operation on https. Certificate location, key and listened port must be specified.<br>**port** — listened port<br>**keystorePass** — a key to a certificate store<br>**keystoreFile** — a store file that contains a certificate<br>**keystoreType** — store type<br>**certAlias** — certificate alias in a store<br>**ciphers** — supported ciphering methods |
| **accessLog** | Server requests logging.<br>**enabled** — logging state<br>**directory** — the directory to store logs<br>**format** — default logs format: NCSA — standard format, custom — expanded format for debugging<br>**append** — current file writing continuation after service restart<br>**retrainDays** — log storage time<br>**append** — additional information<br>**logCookies** — saving cookie to logs<br>**logAP** — saving headers from access points<br>**logBRAS** — saving data from BRAS |
| **database** | |
| **host** | Database server address |
| **port** | The port of the database server for getting inbound connection |
| **name** | Database name |
| **user** | Database user's name |

| | |
|---|---|
| **password** | Database user's password |
| **readOnly** | Database connection status |
| **pool** | Database connections management<br>**connectionTimeout** — the idle timeout of the connection<br>**validationTimeout** — the interval for idle connections validation<br>**min** — the minimum number of connections<br>**max** — the maximum number of connections |
| **cache** | Caching settings<br>**maxEntries** — the maximum number of items in the cache<br>**maxResourceBytes** — cache size<br>**expireTime** — cache data storage time |

### /etc/default/eltex-portal

The file contains parameters needed for service initialization. Default configuration example:

```
# Eltex-Portal daemon parameters

# Port for use by Eltex Portal
PORT=9000

# Initial size of Java heap
JAVA_INIT_HEAP=16m
# Maximum size of Java heap
JAVA_MAX_HEAP=256m

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-portal"
```

| Parameter | Description |
|---|---|
| PORT | The port for the server to get connections. |
| JAVA_INIT_HEAP | Amount of memory allocated for service operation on startup. Recommended to be set equal to JAVA_MAX_HEAP. |
| JAVA_MAX_HEAP | Maximum amount of memory that the service can reserve. |
| JAVA_OPTS | Additional options for jvm launch. |

### /etc/eltex-portal/log4j2.xml

service operation logging settings. Default configuration example

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration monitorInterval="600">
    <properties>
        <Property name="maxFileSize">20 MB</Property>
        <Property name="accumulatedFileSize">100 GB</Property>
        <Property name="lastModified">4d</Property>
        <Property name="maxCount">20</Property>
        <Property name="baseDir">/var/log/eltex-portal</Property>
    </properties>
    <appenders>

        <RollingFile name="RollingFile" fileName="${baseDir}/log_ep.txt"
                     filePattern="${baseDir}/log/log_ep-%i.txt.gz">
            <PatternLayout>
                <pattern>%d{ISO8601} [%t] %-5p %logger{12} %C{1}.%M(line:%L). %m%n</pattern>
            </PatternLayout>
            <Policies>
                <SizeBasedTriggeringPolicy size="${maxFileSize}"/>
            </Policies>
            <DefaultRolloverStrategy max="${maxCount}">
                <Delete basePath="${baseDir}" maxDepth="3">
                    <IfFileName glob="log_ep-*.txt.gz">
                        <IfLastModified age="${lastModified}" />
                        <IfAny>
                            <IfAccumulatedFileCount exceeds="${maxCount}" />
                            <IfAccumulatedFileSize exceeds="${accumulatedFileSize}" />
                        </IfAny>
                    </IfFileName>
                </Delete>
            </DefaultRolloverStrategy>
        </RollingFile>

    </appenders>

    <Loggers>
        <Root>
            <AppenderRef ref="RollingFile" level="WARNING"/>
        </Root>
        <Logger name="org.springframework" level="INFO"/>
        <Logger name="net.sf.ehcache"      level="ERROR"/>
        <Logger name="org.eclipse.jetty"   level="INFO"/>

        <!--SQL logging-->
        <Logger name="org.jooq.tools.LoggerListener" level="OFF"/>

        <Logger name="jndi"       level="OFF"/>
        <Logger name="org.quartz" level="OFF"/>
        <Logger name="com.zaxxer" level="OFF"/>
        <Logger name="org.apache" level="OFF"/>
```

```
    </Loggers>

</configuration>
```

| Parameter | Description |
|---|---|
| monitorInterval | The interval for automatic monitoring of the logger configuration. |
| maxFileSize | The maximum file size. When exceeded, a new file is created, and an old file is archived. |
| accumulatedFileSize | Total log size (a current file + archived ones). When exceeded, the oldest files will be deleted. |
| lastModified | Log storage time, files modified earlier than the timeless, will be deleted. |
| maxCount | The maximum number of archived files. When exceeded, the oldest files will be deleted. |
| baseDir | Base directory to store logs. |
| | |
| <AppenderRef ref="RollingFile" level="ERROR"/> | Minimum logging level. |

## Log errors description

Log file: /var/log/eltex-portal/log_ep.txt

| Browser | Description | Example |
|---|---|---|
| CHECK LOGIN AND PSW IN smsc_gate.conf | NGW failed to access SMS sending service | 2018-08-22T09:38:56,420 [SimpleContainerScope.Executor@266376052-35] ERROR org.eltex.portal.sms.SendSmsWithPswResponseHandler SendSmsWithPswResponseHandler.onResult(line:53). Error while sending message on number: 79529056800. ErrorCode: 10, errMessage: 79529056800. Received error code = 1. CHECK LOGIN AND PSW IN smsc_gate.conf. Error in the parameters of function of dispatch sms via http protocol |
| NGW_NOT_AVAILABLE | The portal failed to access NGW service | |

## v1.14_List of recommended browsers

The list of browsers checked for correct displaying of Eltex Portal on user devices.

### Windows 10 (PC)

| Browser | Version |
|---|---|

| | |
|---|---|
| Mozilla Firefox | 54.0.1 |
| Google Chrome | 59.0.3071.115 |
| Yandex Browser | 17.6.1.743 |
| Microsoft Edge | 40.15063.0.0 |
| Internet Explorer | 11.483.15063.0 |
| Vivaldi | 1.10.867.48 |
| Opera | 46.0.2597.46 |
| Maxthon MX5 | 5.0.4.3000 |
| K-Meleon | 76 Pro "Eu Genia" |
| SRWare Iron | 58.0.3050.0 |
| SlimJet | 15.0.2.0 |
| Amigo | 56.0.2924.197 |
| Chromium | 61.0.3158.0 |

### MAC OS

| Browser | Version |
|---|---|
| Safari | 9.1.3 |
| Google Chrome | 59.0.3071.115 |
| Opera | 45.0.2552.888 |
| Mozilla Firefox | 53.0.3 |

### Android

| Browser | Version |
|---|---|
| Google Chrome | 59.0.3071.125 |
| Mozilla Firefox | 54.0.1 |
| Opera | 42.8.2246.118317 |
| Dolphin | 11.4.17 |
| UC Browser | 11.3.8.976 |
| CM Browser | 5.21.08 |
| Next Browser | 2.17 |
| Maxthon | 4.5.10 Build 2959 |

### iOS

| Browser | Version |
|---|---|

| | |
|---|---|
| Safari | 10.3 |

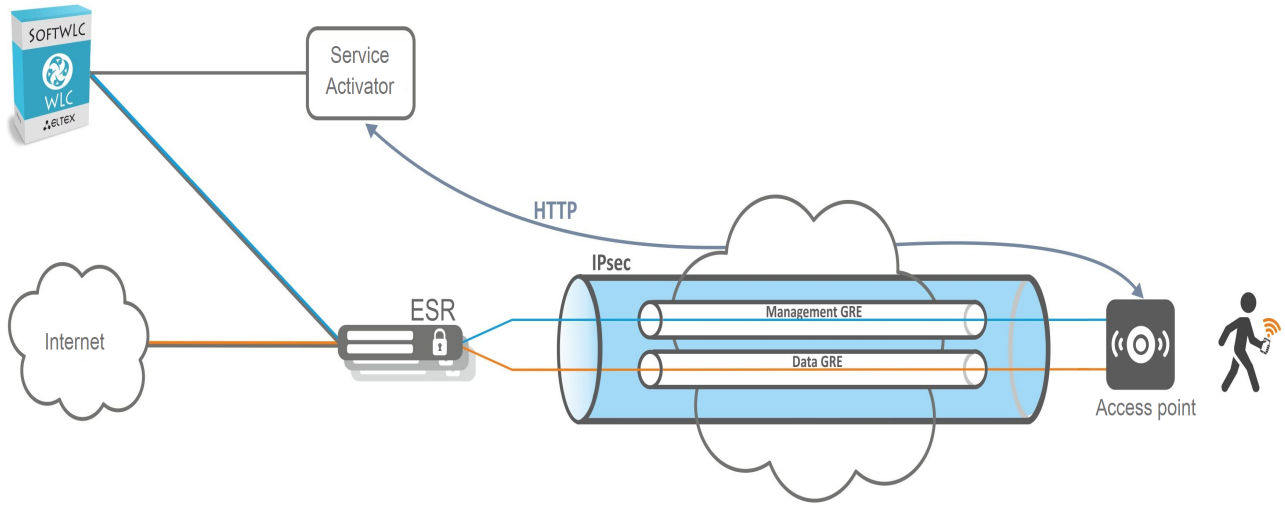
**Windows Phone 10**

| Browser | Version |
|---|---|
| Microsoft Edge | 40.15063.483.0 |
| UC Browse | 4.2.1.541 |

## v1.14_OTT (EN)


- General scheme
- Quickstart
- General description
  - Service Activator
    - Automatic activation of the service with default settings
    - Service Activator performance chart
    - Configuration files
    - Minimum requirements for the server of the Service Activator.
    - Installing the Service Activator
- ESR
  - Redundancy
  - ESR connection scheme
  - ESR redundancy scheme
- Access points
- Use case
- Message exchange diagram
- Configuration
  - AP initialization
  - ESR OTT
    - Configuring IPsec on AP without the Service Activator
  - OTT black list
  - Deleting OTT link
  - Shaper settings via the Admin Panel
  - NBI for OTT management
- Annex 1. List of IPsec parameters in the OTT profile
- Annex 2. Description of errors returned by the Service Activator to access points
- Annex 3. ESR configuration example
- Troubleshooting
  - Service Activator logs
  - Viewing OTT information on access points
  - Manual starting of the Service Activator's client part on an AP with debug enabled

## General scheme




## Quickstart

1. Install SoftWLC and the Service Activator:
2. In the file /etc/eltex-wifi-sa/factory-fw.conf, adjust firmware versions for a version of the AP being installed to be consistent with them. Set the Downgrade parameter to false. Download AP firmware to the /var/lib/eltex-wifi-sa/firmware/ directory and rename it according to the name of the file specified in /etc/eltex-wifi-sa/factory-fw.conf.
3. Download the Root certificate and the certificate of the Service Activator to the directory /etc/eltex-wifi-sa/.
4. Edit the names of the Root and the Service Activator certificates in the file /etc/eltex-wifi-sa/application.conf. Set the parameter CheckMAC to Yes. Restart the Service Activator: service eltex-wifi-sa restart.
5. Create a domain for ESR and a subdomain for OTT access points.
6. Create an initialization rule for the required AP model. TCP protocol should necessarily be specified as SNMP transport (see AP initialization).
7. Create an initialization rule link to an OTT access point. In the link, the "Connected" checkbox should be set (see AP initialization).
8. Create an OTT profile with IPsec parameters. The password specified in ESR configuration, for example, "testing 123", should be taken as the "IPsec password". The command CreateOttProfile should be run in NBI (see ESR OTT).
9. Add ESR to the EMS domain for OTT access points. Set OTT checkbox in the Access tab to ServiceProvider and enable the BRAS checkbox. Make sure that ESR is accessible from SoftWLC (see ESR OTT).
10. In the NAS table (the tab RADIUS - Access Points), edit a password for RADIUS ESR that is specified in its configuration, for example "testing123".
11. In the ESR tab of ESR configuration, specify ESR public IP and select an OTT profile. The command CreateOttStation should be run in NBI (see ESR OTT).
12. Create a SSID and link it to an OTT domain. In SSID parameters, specify the Location set in ESR configuration, for example, "testing2" (see AP initialization).

13. In the Admin Panel, in the "System" tab of Settings menu, enable the checkbox "Shaper settings at Domains tree", exit the Admin Panel and enter it again (see Shaper settings in the Admin Panel).
14. After that, enable the shaper on SSID in the "Domains tree" tab of the Settings menu (see Shaper settings in the Admin Panel).

## General description

### Service Activator

The Service Activator is a server based on x86 architecture and Ubuntu 14.04 operating system with a special software installed. Its task is to receive and process POST HTTPs requests from access points and to exchange information with SoftWLC. In terms of programming, the Service Activator is a WEB server. To get requests from access points, the Service Activator should have open port 8043 and a public IP address. As access points will refer to the Service Activator by its URL, it is necessary to provide a link between the Service Activator's public address and its domain name on DNS servers. Another network interface of the Service Activator should be linked to an EMS module, i.e., it should be put into a single address space of SoftWLC modules. To provide security, traffic between the Service Activator and EMS should pass through the firewall. To provide communication between the Service Activator and SoftWLC, port 8080 (HTTP) used by the Service Activator to request EMS, should be opened on the firewall.
The Service Activator can be located behind the proxy server (in relation to the Internet) and have a private IP address to communicate with access points. Therefore, the proxy server should send POST requests to the Service Activator with or without replacing a TCP port. In Service Activator configuration files, the number of a TCP port listened by the server can be specified.
Once an access point has sent an HTTPs request containing its data to the Service Activator, the last one checks the access point certificate. To do this, the Service Activator should have the Root certificate and the Service Activator certificate (containing Provider-ID) signed by it. Provider-ID – service provider identifier. It is used to make access points that belong to a certain provider connect only to this provider's Service Activator. The Service Activator can optionally check the consistency between an access point's MAC address specified in a certificate and its real MAC address. It protects a provider from certificate theft by one access point and its usage by another one. If certificate check, handshake and other procedures has been successful, the Service Activator proceeds to verification of AP firmware relevance. The correspondence between relevant firmware versions and models of access points is stored in the */etc/eltex-wifi-sa/factory-fw.conf* configuration file. If the firmware version of the access point requesting the Service Activator differs from the version specified in this file, the Service Activator gives an access point an order to update its firmware. I.e., firmware files for access point models used should be placed on the Service Activator in advance.
If a firmware file is not placed on a server activator, or if an access point's firmware version corresponds to the current version specified on the Service Activator, it proceeds to searching for an initialization rule link in the database. If there are no links, the Service Activator puts the AP into a "sandbox" until a link is found.

> Access points' firmware downgrade can be disabled. Then only those access points that have firmware version lower than the one specified on the Service Activator will be subject to update.

Before linking an access point, 2 objects should be created in a system:

1. **OTT profile.** The profile contains a big number of IPsec settings according to which access points and ESR will create IPsec tunnels. IPsec parameters available in OTT profile are listed in Annex 1. In NBI, this profile can be created by using the *CreateOttProfile* command.
2. **Linking OTT profile to ESR**. Linking ESR public IP addresses to OTT profile created before. As a result, IPsec parameters from OTT profile are compared with ones specified by ESR. Then, when the Service Activator chooses ESR for an access point, it will send its public address and IPsec parameters to the AP. As a result, the same IPsec parameters will be guaranteed if a tunnel is established both on the access point and on ESR side. IPsec parameters set on ESR by profile linking, can be optionally adjusted in ESR configuration. In NBI, linking OTT profile to ESR can be created by using the *CreateOttStation* command.

To implement OTT profile linking to ESR and for the Service Activator to choose ESR for an access point, ESR devices should be added to EMS device tree in advance. OTT checkboxes should be enabled on ESR devices in the Service Provider mode to show their readiness to work with access points according to OTT model. In addition, public IP addresses should be configured on them. ESR devices should be put into the domains where they will be initialized according to OTT AP initialization rules links. Access points can also be initialized in subdomains of the domain where ESR is located.
After all objects has been created, it is necessary to perform MAC linking of the access point to the initialization rule. OTT checkbox in the Links menu should be set to Connected. A domain where ESR OTT is located or its lower-level subdomain should be selected as Node domain.
After the link to initialization rule has been created, the Service Activator selects ESR for the AP to establish an IPsec tunnel to using the following algorithm: the Service Activator starts searching for ESR with the OTT checkbox set in a domain where an AP is located according to the initialization rule link. If there is no such ESR devices in the current domain, the algorithm goes one level higher in a domain tree and continues to go up until OTT ESR is found. If OTT ESR is not found, the Service Activator will return error 4022. The Service Activator selects the ESR for which the load and the number of connected access points are lower at the moment. After that, the Service Activator generates a unique login and password for X-Auth Authorization and sends a resulting message including ESR public IP, IPsec parameters set in ESR configuration and credentials for X-Auth.

> ⓘ To provide seamless roaming between access points, connect them to the same ESR. According to the ESR selection algorithm, if an access point is put into a domain where other access points are already put, priority is given to the ESR to which those points are connected.

Automatic activation of the service with default settings

On the Service Activator, there is a possibility to add access points to default domains. This option is necessary if a default Wi-Fi service should be activated on an access point right after its installation without participation of an operator and links to initialization rules. To do this, create the "ott.root" domain in the system and add a link to initialization rule of "ott_default" key to the domain of the "ott.root" node. Link SSID to the domain. Link the portal that will be accessible to all users that connect to an access point put into the default domain to SSID. ESR devices with enabled OTT checkboxes and linked OTT profiles should be put into the domain.
After this sequence of operations has been performed, the connection algorithm will be as follows:

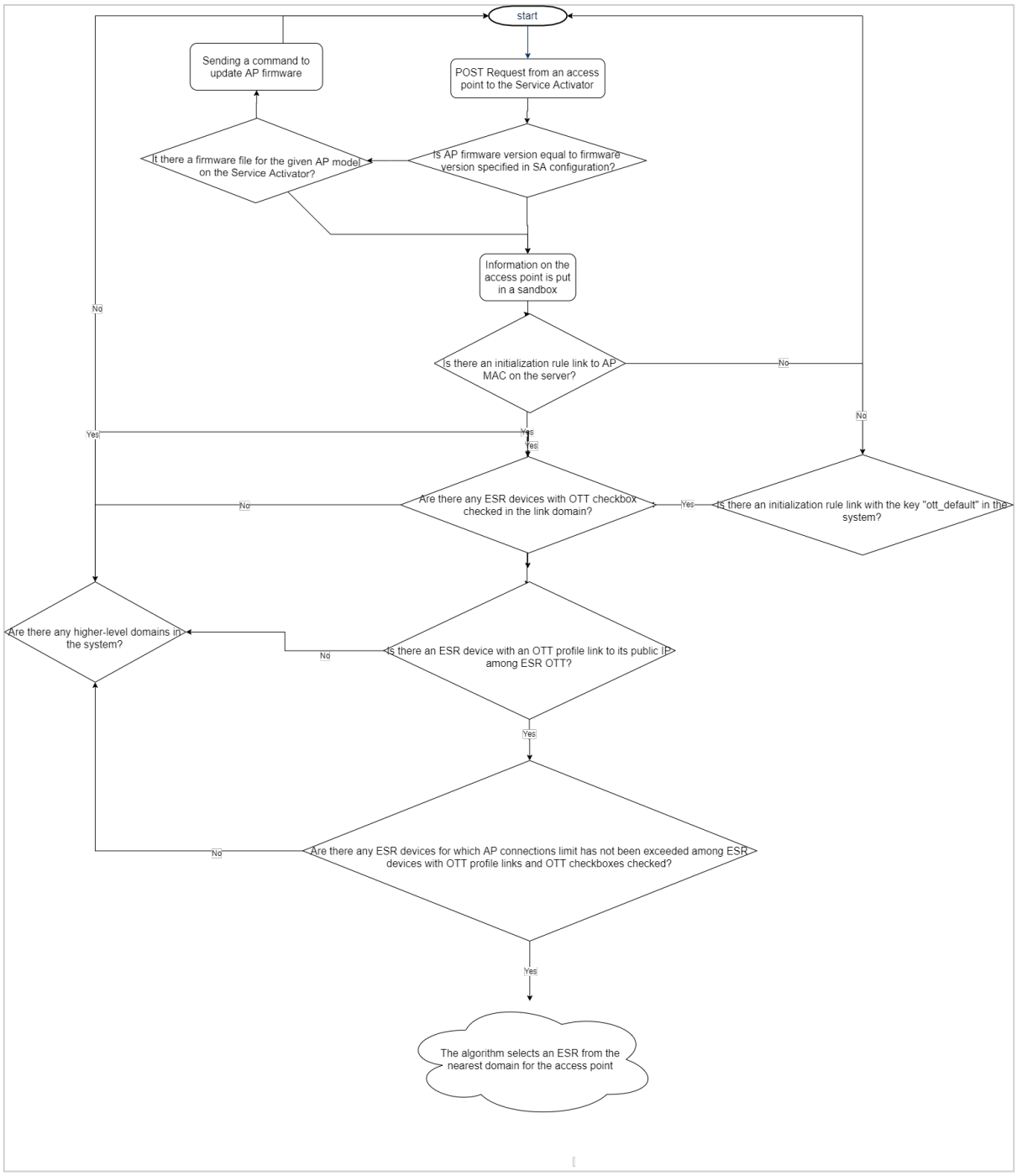
- After being installed, the access point will send a POST request containing its parameters to the Service Activator.

- If the Service Activator does not find a link to initialization rule by the AP's MAC address, it will put this access point into the default domain and start searching for an optimal ESR in that domain.
- A message containing parameters required for establishing an IPsec tunnel will be sent to an access point.
- An access point will establish tunnels and connect to SoftWLC. After that, an access point will be initialized, and SSID, linked to the default domain, will be enabled on it.

As a result, a default service will be enabled on the access point automatically, without operator intervention.

When the defaul domain is used, all client access points for which links to initialization rules by MAC address are not set will be put into the default domain. Nevertheless, from a system perspective, there will be no identifiers that show that an access point belongs to a certain client. Consequently, all statistics and other information on the AP and users connected to it will not be identified by belonging to a client or filtered by client attribute. To link an AP to a certain client, it is necessary to create links of AP initialization rules by MAC to a client's domain, remove the AP from the default domain and initialize it again. When enabling the default domain, an operator takes the responsibility for control over access points and services within the default domain.

Service Activator performance chart




Configuration files

Service Activator configuration files are located in the "/etc/eltex-wifi-sa/" directory. To apply the changes to configuration files, restart the Service Activator using the following command: "service eltex-wifi-sa restart".
Description of the parameters set in configuration files:

**Configuration file "application.conf".**
This file contains most of Service Activator configuration.

| Parameter | Values | Recommended value | Description |
|---|---|---|---|
| logLevel | debug, info, warn, error | info | Logging level. Logs are written to the file /var/log/eltex-wifi-sa/main.log. |
| requestTimeout | integer | 45 | Maximum request processing time (0 for infinite time).<br>If the value of the parameter is exceeded, the server is considered as overloaded. |
| http { enabled | yes, no | true | Enabling request reception from access points via HTTP protocol. |
| http { port | integer (0-65535) | 8042 | The number of TCP port which will be used by the Service Activator to listen to requests from access points via HTTP. |
| https { enabled | yes, no | true | Enabling request reception from access points via HTTP protocol. |
| https { port | integer (0-65535) | 8043 | The number of TCP port that will be used by the Service Activator to listen to requests from access points via HTTPs. |
| https { keyStore { path | string | server.p12 | Service Activator certificate path. If the certificate and the configuration file are located in the same directory, it is sufficient to enter the certificate's name. |
| https { keyStore { password | string | "" | Password for Service Activator's certificate. In most cases, it is an empty string. |
| https { clients { certificate | string | client.crt | Root certificate path. If the certificate and the configuration file are located in the same directory, it is sufficient to enter the certificate's name. |
| https { clients { checkMAC | yes, no | yes | Enabling MAC address checking on the certificate sent by an access point. |
| https { clients { fwCheckCrt | yes, no | yes | Enabling ProviderID checking on a certificate sent by an access point. |
| ems { host | localhost or IP address | | The address of EMS server with which the Service Activator interacts. |
| ems { port | integer (0-65535) | 8080 | The number of a port that is used by the Service Activator to address EMS. |
| ems { parallelLimit | integer | 5 | The maximim number of parallel requests to EMS server |
| ipsec-activator { wait-timer | integer | 180 | Timeout during which an AP tries to set an IPsec connection. After the timeout, an AP is reset. |

| | | | |
|---|---|---|---|
| ipsec-activator { update-time | integer | 600 | Timeout during which an AP tries to update firmware with the Service Acrivator. After the timeout, an AP is reset. |

**Configuration file "factory-fw.conf"**

The file contains settings for automatic AP firmware upgrade to current versions.

| Parameter | Values | Recommended value | Description |
|---|---|---|---|
| downgrade | true, false | false | Permits\forbids AP downgrade if firmware version does not match the version specified in configuration |
| min | string | | The current AP firmware version |
| file | string | | Firmware file located in /var/lib/eltex-wifi-sa/firmware/ |

**Configuration file /usr/lib/eltex-radius-nbi/conf/ott/ott.xml**

This file contains information on the maximum number of OTT access points that can be connected to ESR of this model. When an AP requests to the Service Activator, it finds an ESR OTT device in a domain and checks the number of access points linked to it. If the number is equal or greater than the number specified in the file for this model of ESR, the Service Activator considers it as loaded to its maximum and starts to search a less busy ESR in this domain or in higher-level domains.

| Parameter | Values | Recommended value | Description |
|---|---|---|---|
| subtype | 100, 200, 1000, 1200, 1700 | | ESR model (ESR-100, ESR-200, ESR-1000, ESR-1200, ESR-1700) |
| max | | | The maximum number of OTT access points for the ESR |
| param name, default, regex, description | | | Parameter's name, default value, regular expression and description of parameters available in OTT profile. |

Minimum requirements for the server of the Service Activator.

- CPU 2 Core
- RAM 8GB
- HDD 100GB (до 5000 ТД)

### Installing the Service Activator

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# echo "deb http://archive.eltex.org/ems 3.13 main" >> /etc/apt/sources.list.d/eltex.list
root@vagrant-ubuntu-trusty-64:/home/vagrant# add-apt-repository -y ppa:webupd8team/java
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-key adv --keyserver keyserver.ubuntu.com --recv F558A287
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get update
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get -y install oracle-java8-installer
root@vagrant-ubuntu-trusty-64:/home/vagrant# apt-get install eltex-wifi-sa
```

If the Service Activator is installed to a separate server, specify EMS server access parameters in the configuration file /etc/eltex-wifi-sa/application.conf and restart the Service Activator:

```
ems {
host = "localhost"
port = 8080
```

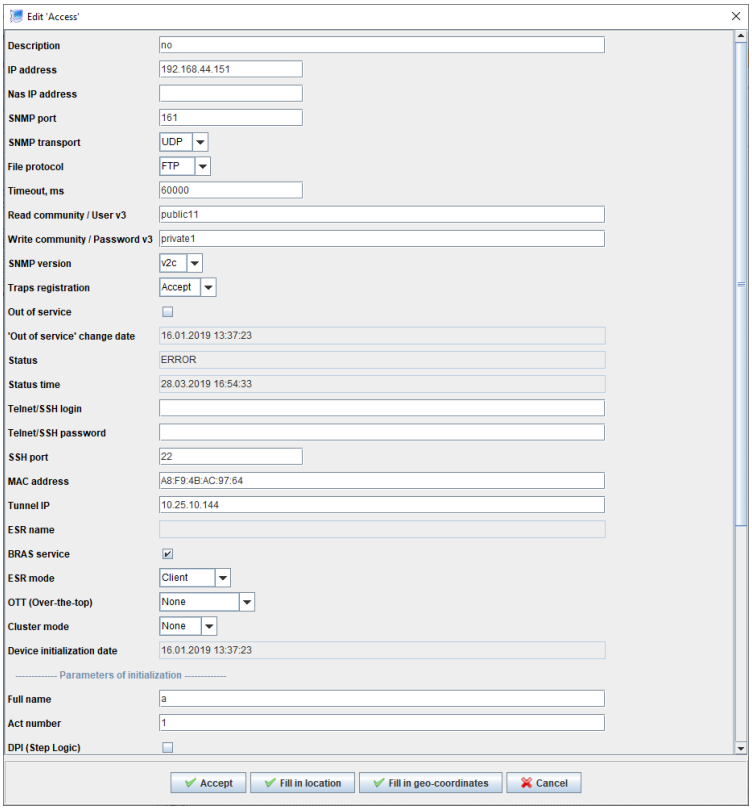
## ESR

To provide the OTT service, ESR should have 2 default gateways to send traffic to the Internet. The first gateway is specified as a standard Default Gateway in the routing table. ESR uses it to transmit IPsec packets. ESR should have an interface with a public IP address in this subnet. Access points will establish IPsec tunnels to this IP address, so ports 500 and 4500 should be opened. ESR uses the second gateway to send subscriber traffic extracted from tunnels. To prevent the problem of 2 default gateways within the same routing space, configure the option Next-Hop on the Bridge. The Bridge is a gateway for subscriber traffic that this traffic is routed through. The option allows routing all traffic from the Bridge via a gateway specified in the option Next-Hop bypassing the Default Gateway.
During establishing IPsec sessions, X-Auth authorization is performed. ESR receives unique login and password (generated by the Service Activator) from the AP and performs authorization by sending RADIUS requests to SoftWLC PCRF. When connected to MongoDB, PCRF informs ESR on match between login and password sent by the AP and ones stored in the database.

### Redundancy

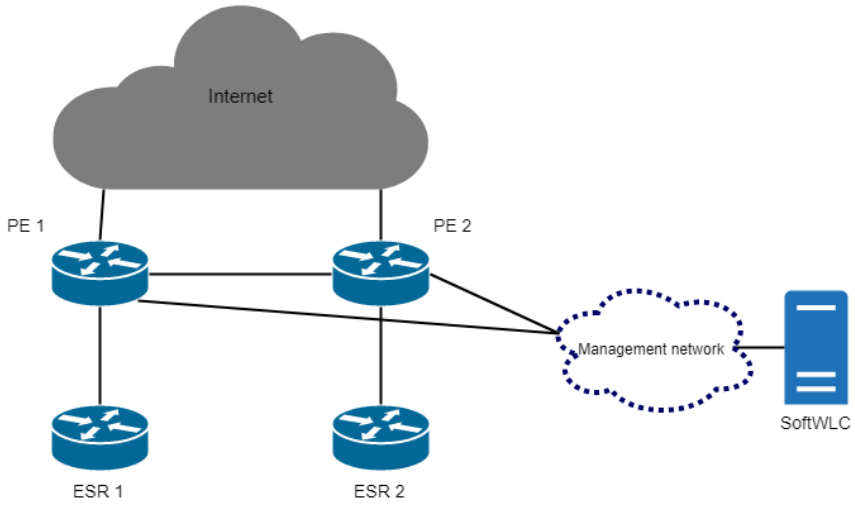
ESR redundancy is provided according to N+1 model. In the case of a failure in a domain of one of the ESR devices and IPsec session abort, access points send information regarding the need to get data for connecting to another ESR, to the Service Activator. The Service Activator sends information on other ESR devices taking failures and device loads into account. As a result, access points are connected to other ESR devices instead of the failed ESR. This redundancy scheme allows reducing the number of ESR devices in the network.
When one of ESR devices fails, and its access points are connected to the Service Activator, it starts to search for a new ESR for these APs within the same domain. If there are no free ESR devices in this domain, or there are not any, the Service Activator goes one level higher in the domain tree and continues to search for ESR there. If there are no free ESR devices, the Service Activator goes one level higher and so on. Therefore, it would be useful to create several ESR groups and put them into different regional domains. Access points of these regions will be connected to their regional ESR devices. Thus, the way data move from an AP to ESR will be limited to a specific region. In this case, one more group can be put into the root of OTT branch. If all ESR devices in the region fail or become unavailable for some reason, access points will be able to switch to root ESR devices. The length of the route that packets travel will increase if root ESR devices and access points are located in different regions, but the service will be provided. Regional and root ESR devices can be linked to different OTT profiles with different IPsec parameters, and AP distribution will be correct, as an access point always gets from the Service Activator precisely those IPsec parameters that are confugured on the ESR the AP is connected to.

ESR connection scheme




1. One interface is physically used.
2. The interface bridge 1 is used to access the Internet. Traffic goes via this interface on the default route.
3. IPsec listens to inbound connections via bridge 1.
4. IPsec from an AP is unpacked on bridge 1. GRE packets are redirected to bridge 2.
5. Then packets from AP management VLAN are transferred to bridge 6.
6. Client traffic comes to bridge 7 and is sent to a neighbouring router according to the option route-map. Clients will access the Internet via that router.

ESR redundancy scheme




1. Routers ESR 1 and ESR 2 on which IPsec is terminated are connected to routers PE 1 and PE 2 respectively.
2. ESR 1 and ESR 2 announce management, client and IPsec gateway subnets to PE 1 and PE 2 respectively, using BGP.
3. PE 1 and PE 2 announce default routes and subnets necessary to provide communication with SoftWLC.
4. If one ESR fails, it becomes unavailable. When access points understand that IPsec connection cannot be established, they request the Service Activator that gets information on failure of one of ESR devices and sends parameters to access points for them to be able to connect the second ESR. Access points are connected to the new ESR.
5. Each ESR uses own IP address pools to control access points and Wi-Fi users.

ESR configuration example can be found in Annex 3.

## Access points

According to the OTT model, an access point should connect to the Service Activator, get IPsec parameters and authorization data before IPsec tunnel establishing. As connection method should be secure, HTTPs should be used. HTTPs requires certificates located both on the AP and on the Service Activator. To do this, specify URL of a Service Activator to which the AP will send a request. This can be done in two ways:
1) If a service provider entered into a contract with Eltex, a specially prepared certificate that contains unique parameter "Provider-ID" and Service Activator URL, which an AP will address to, can be embedded within access points' firmware at the manufacturing stage. Consequently, this URL should be agreed in advance between a vendor and a provider. As a result, a provider gets access points that will be automatically connected to the Service Activator using URLs from their certificates when installed. A service provider will be given the Service Activator certificate and the Root certificate. The Service Activator certificate also contains "Provider-ID" used by the Service Activator to check if a requesting access point belongs to a provider. If it does not, a request will be ignored. In this case, an installer does not need to configure anything to enable the service.
2) If a service provider has not entered into a contract with Eltex for manufacturing access points with unique Provider-ID, access points with default Provider ID = "eltex" and empty Service Activator URL are manufactured. As long as Service Activator's URL is empty, an access point operates as a standard AP (OTT is disabled). To enable OTT, specify Service Activator's URL via CLI or AP WEB interface. An AP will

try to connect to the Service Activator. The Root and the Service Activator certificate with Provider-ID = "eltex" are given to a provider. All access points with this Provider-ID will be able to connect to the Service Activator if its URL is specified on them. If a link to an initialization rule is not created, the access point will be put into a "sandbox and will not reach the system. Due to this restriction, "alien" access points will not be able to get a provider's service.

All AP certificates contain MAC addresses of these access points. When the Service Activator gets a request from an access point, it can optionally check a MAC address specified in the certificate and an actual address of an access point. If they differ, the Service Activator will generate an error and will not let it pass to the next activation steps. This procedure protects a provider from certificate theft by one access point and its usage by another access point with another MAC.

For access points to work according OTT model, an installer adapted to this mode should be embedded into access points' firmware. The installer can be embedded into an access point's firmware only within Eltex manufacturing process. Thus, the OTT model is supported only by Eltex new access points that have passed an appropriate manufacturing stage. A provider can get access points with support of OTT model by making a special order via Eltex commercial department.

If an access point operates on the OTT model (Service Activator URL is specified on the access point), but the access point gets DHCP option 43 with a primary IP address, OTT is disabled on this AP. The access point starts working in a standard mode.

If a failure occurs on ESR-1000, an access point will reset and request the Service Activator after the period:
`(GRE_ping_counter x 10) + waite_timer,`
where `GRE_ping_counter` is a parameter in OTT profile, waite_timer is a Service Activator parameter. By default, this time is 3x10 + 180 = 210 seconds.

## Use case

1) An installer sets an Eltex access point with firmware customized for a service provider at a client's. This firmware contains URL of provider's Service Activator by default. The Service Activator is installed to separate servers of a provider's data processing centre and is a part of SoftWLC. It has a public IP address for AP connection and a domain name specified on a provider's DNS.
2) The access point gets IP address (via DHCP), other network parameters and Internet access from local network. If the access point has received DHCP option 43, it is located in a provider's network, and IPsec establishment is not required. The access point will be guided by suboptions of option 43 and will not start OTT. If the access point has not received option 43, it will start OTT.
3) An access point connects to the Service Activator via HTPPs and transmits the following data:

- Serial number
- MAC address
- Firmware version
- HW version

- Provider-ID (in a certificate)
- MAC-address (in a certificate)

4) When the Service Activator gets a request from an access point, it connects to EMS via NBI, transmits the received data and requests for initialization rule links to this AP (in case if Provider-ID is consistent with AP MAC address specified in the certificate, and handshake is successful).
5) Several options are possible then:

- If the access point was linked to an initialization rule by an operator in advance, and the installer set this access point, initialization will start immediately.
- If the access point is not linked to an initialization rule at the time of its installation, and there is no link of an initialization rule to the default domain, EMS will put the AP to its "sandbox". The AP will be displayed like all other access points. At certain intervals, the access point will try to connect to the Service Activator, waiting for configuration in the system.
- If the access point is not linked to an initialization rule at the time of its installation, and there is a link of an initialization rule to the default OTT domain, the access point will be linked to the default OTT domain. It will be initialized similarly to the access point that has a link to an initialization rule by MAC (but within the OTT default domain and without definition of belonging to a client).
- The access point is added to the black list, so it will not get into the "sandbox".

6) For the access point to establish an IPsec tunnel, create a link of an iniatialization rule to its MAC address via EMS. The operator should enable the OTT connection indicator before including it to the network. Besides the checkbox, the AP domain is an important parameter. EMS sends the AP domain and the OTT indicator to the Service Activator in response to requests. If the default OTT domain is enabled in the system, this step can be skipped.
7) When EMS gets data on the access point, it performs the following actions:

- It finds a level where ESR-1000 pool is based in the domain chain. Therefore, ESR-1000 devices with their IP addresses should be specified in a special domain in EMS.
- EMS generates unique login and password for establishing an encrypted IPsec connection and adds them to the database (MongoDB ott.xauth).
- EMS sends the following parameters upon enquiry: public IP address of a chosen ESR device, login and password (x-auth), the default password (it is the same for ESR-1000 and all access points and is specified in a system only once, as it is necessary for IPsec session establishment), IPsec ESR parameters.
- The Service Activator sends the parameters to the access point.

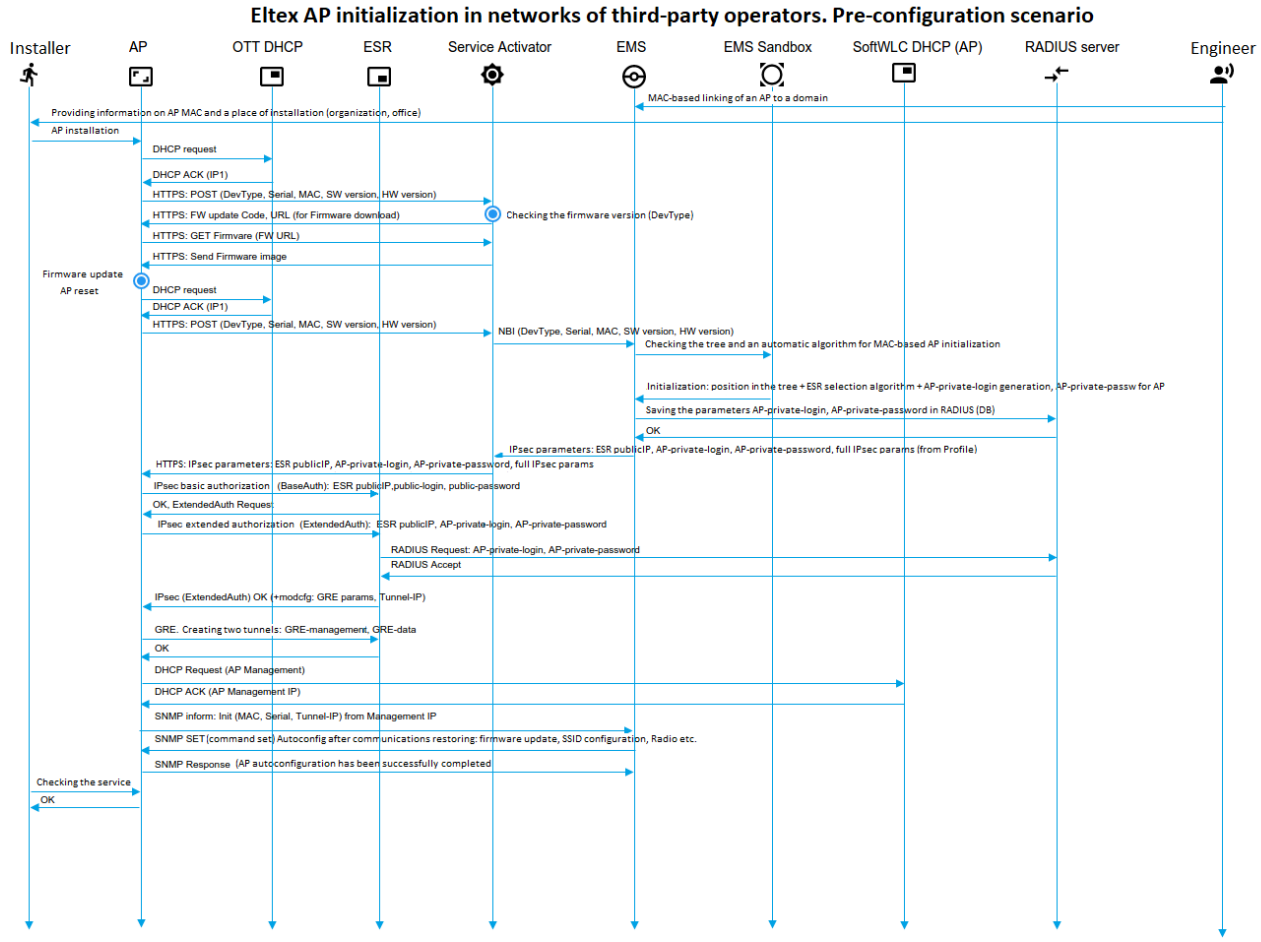
8) After receiving necessary data, the access point starts establishing an IPsec tunnel to ESR-1000. During IPsec connection establishing, ESR-1000 receives unique login and password from the access point and checks them on SoftWLC PCRF server. PCRF connects to the ott database and checks if the table contains login and password received from the access point. If these login and password are in the table. RADIUS sends access-accept.
During IPsec installation, the access point gets a second IP address and other parameters within the IPsec session. This IP address is used by the access point to establish EoGRE tunnels (Management and Data) to ESR-1000 within an IPsec tunnel.

To see the table referred to by RADIUS, do the following:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# mongo>
> show databases;
local    0.078125GB
notification-gw    0.203125GB
ott    0.203125GB
pcrf    0.453125GB
wifi-customer-cab    0.203125GB
> use ott
> show tables
system.indexes
xauth
> db.xauth.find()
{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854d"), "ipsec_login" : "login1",
"ipsec_pass" : "password1" }
{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854e"), "ipsec_login" : "login2",
"ipsec_pass" : "password2" }
{ "_id" : ObjectId("5a6816b4e14c08c4d9c0854f"), "ipsec_login" : "login3",
"ipsec_pass" : "password3" }
```

9) The access point communicates with SoftWLC via SNMP within the Management GRE and is initialized similarly to the current scheme.
10) Subscriber traffic passes through Data GRE to ESR-1000 and is routed to NAT.

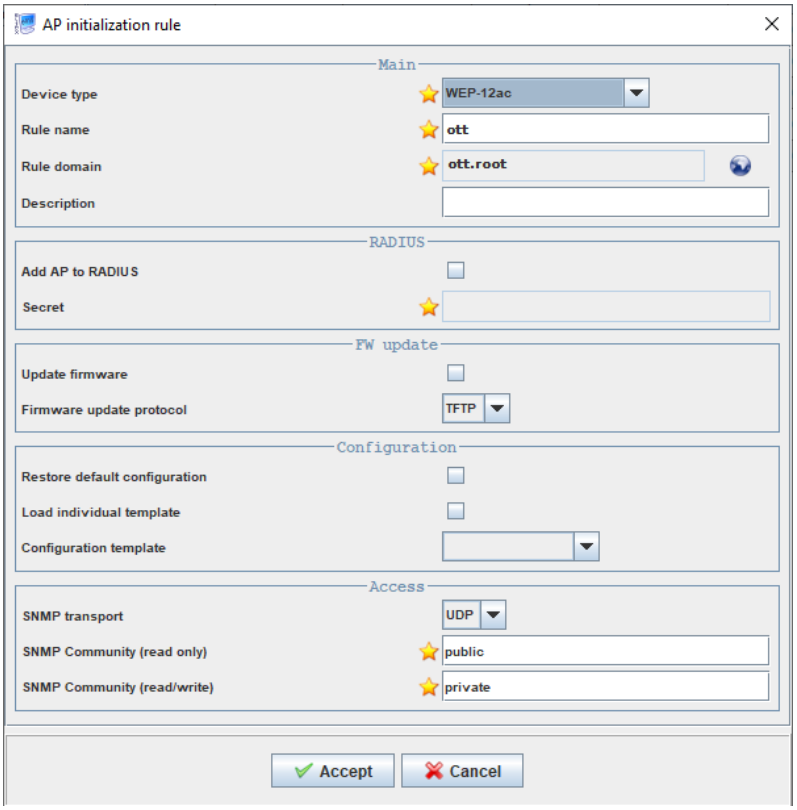
## Message exchange diagram



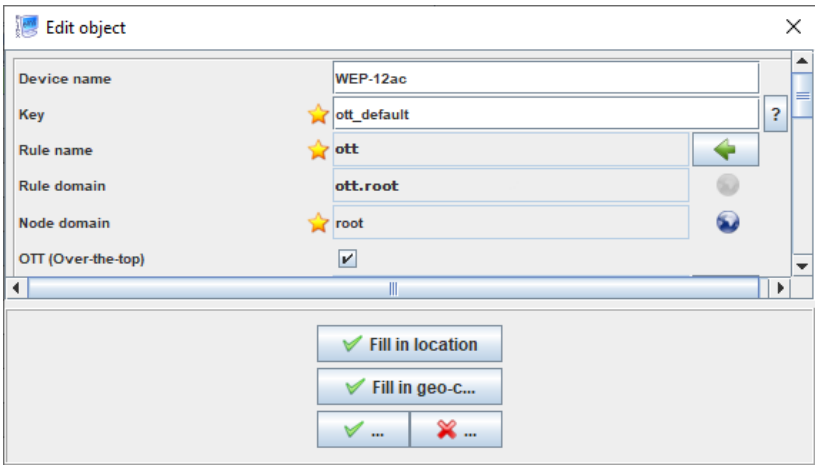

## Configuration

### AP initialization

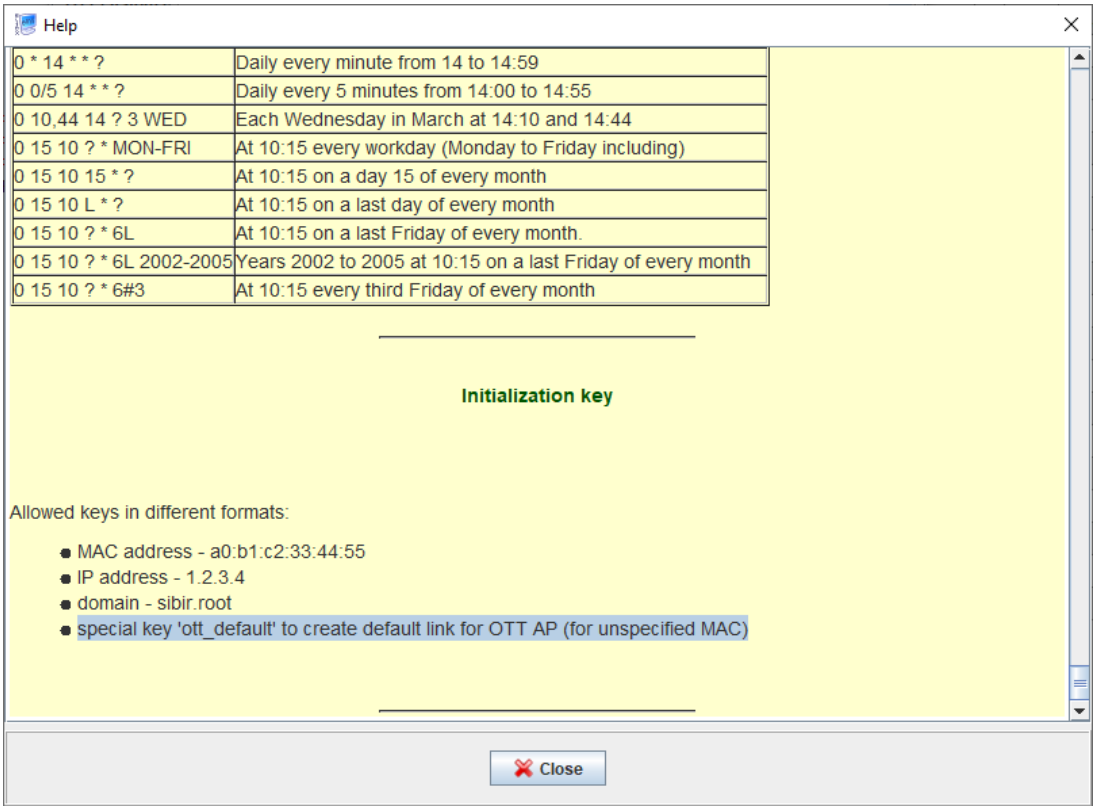
To initialize access points connected according OTT scheme, create the domain *ott.root* in the EMS tree. Create an *OTT* rule in the tab Wireless/AP initialization rules manager/Rules. *OTT* initialization rule can be created manually for each type. Specify TCP as SNMP transport.



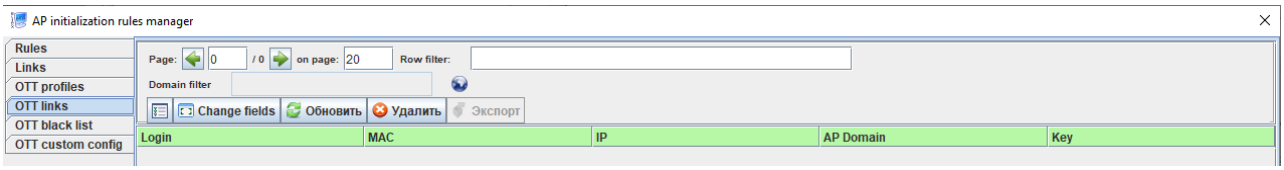

Create an initialization link with ***ott_default*** key, *ott* rule name and *ott.root* domain.



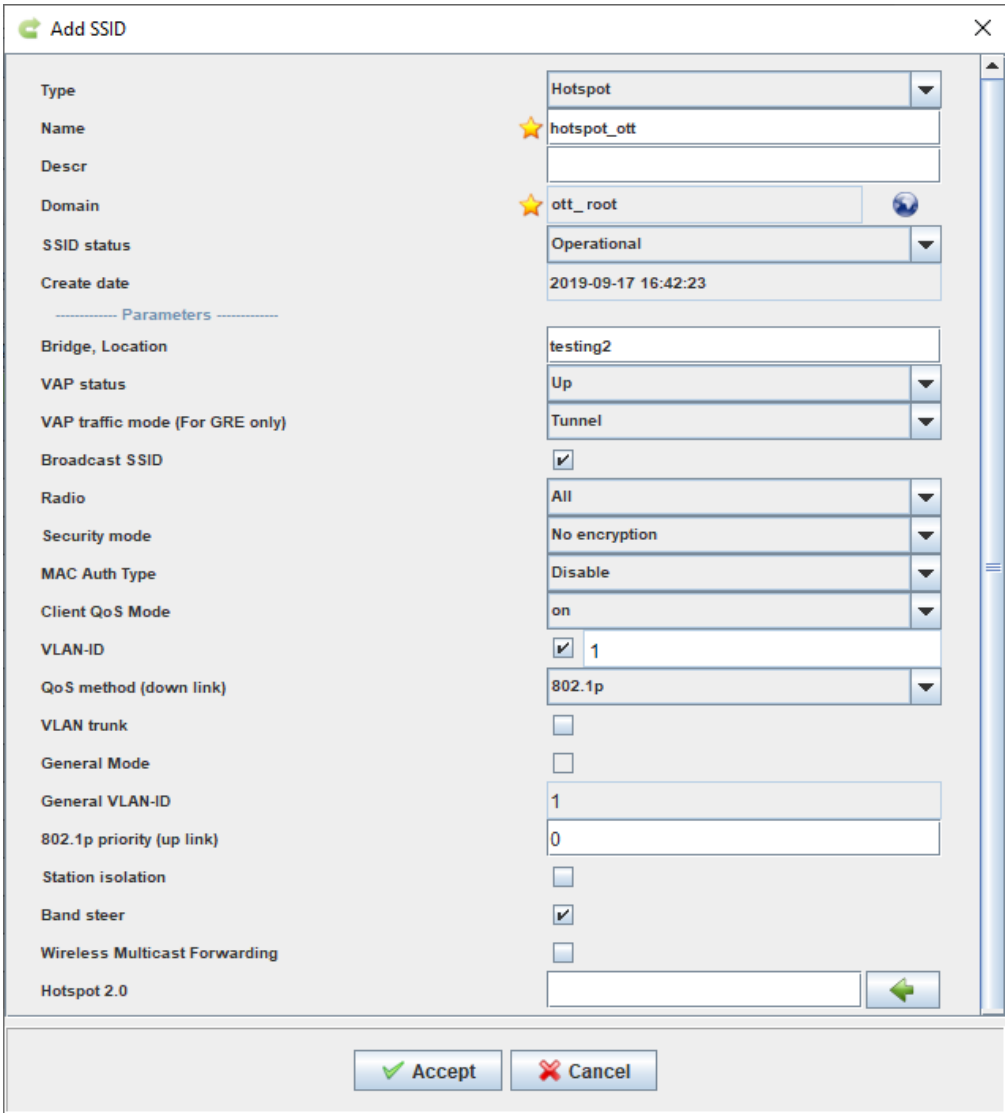

Special key *ott_default* can be obtained by pressing the button 

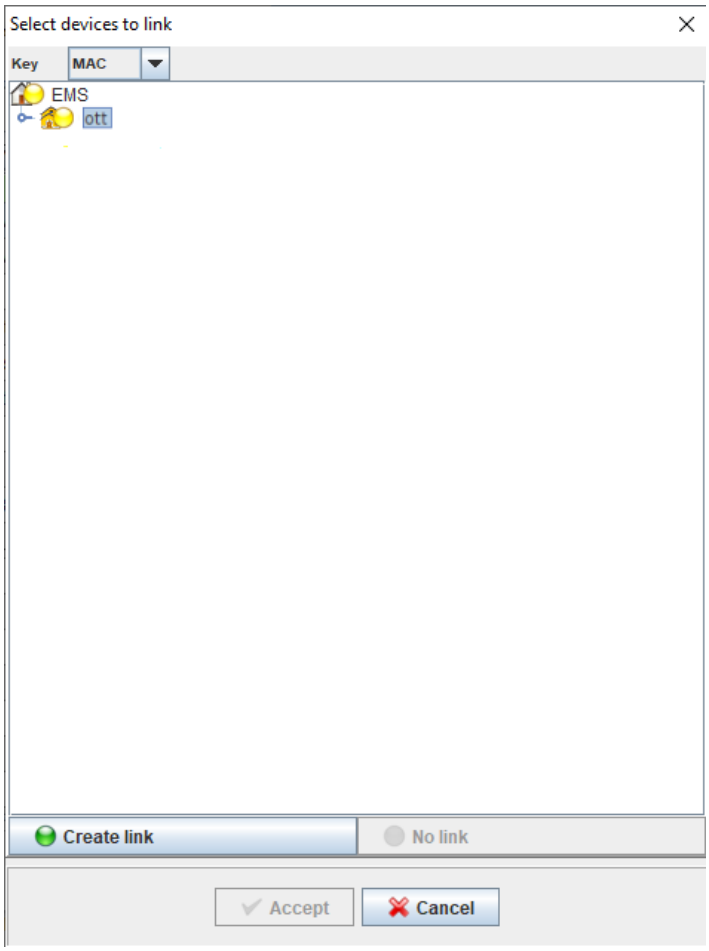



After the link is created, it will be displayed in the tab *OTT links* in Wireless/AP initialization rule manager.



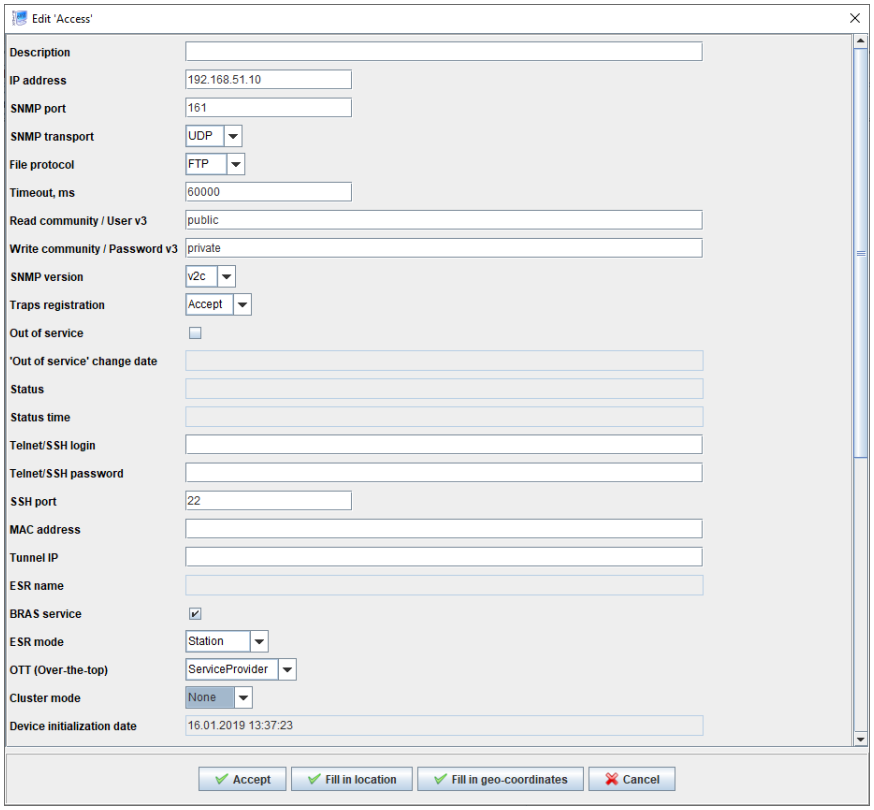

Create a SSID with a link to the domain ott.root (Wireless/SSID Manager). In the field *Bridge, Location* specify the location corresponding to bridge settings on ESR.


Add SSID
Type
Hotspot
Name
hotspot_ott
Descr
Domain
ott_ root
SSID status
Operational
Create date
2019-09-17 16:42:23
---------- Parameters ----------
Bridge, Location
testing2
VAP status
Up
VAP traffic mode (For GRE only)
Tunnel
Broadcast SSID
Radio
All
Security mode
No encryption
MAC Auth Type
Disable
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
Wireless Multicast Forwarding
Hotspot 2.0
Accept
Cancel

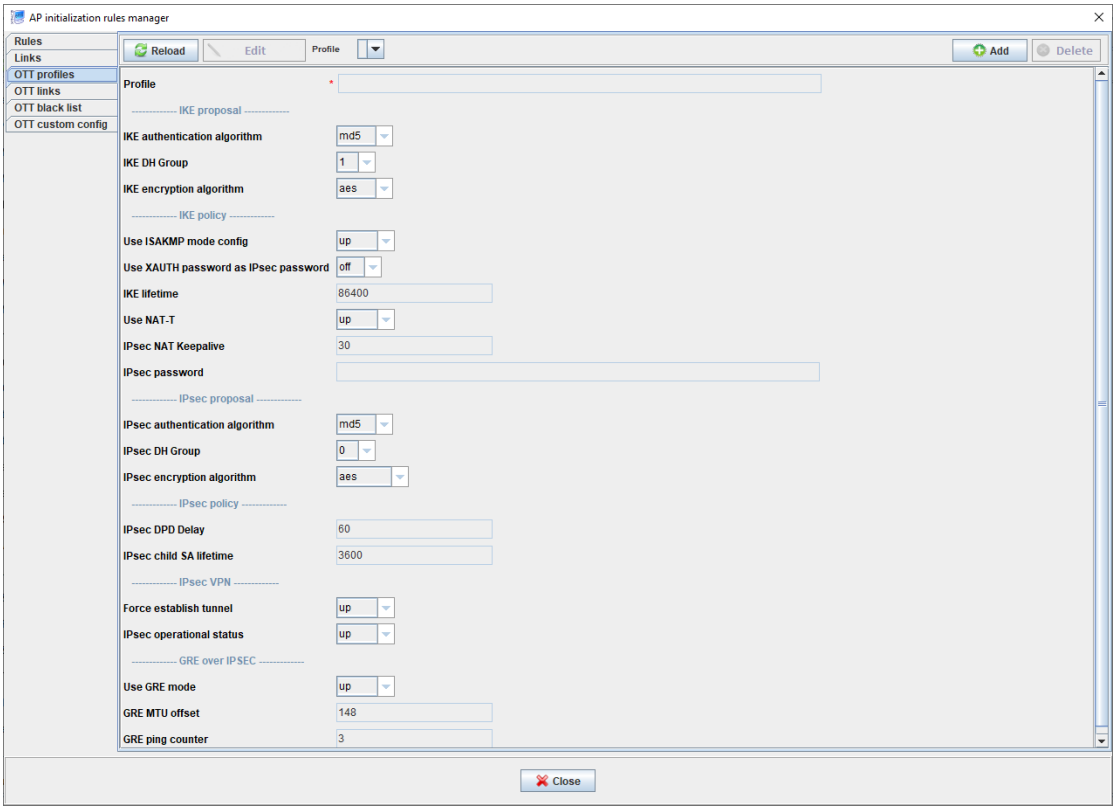



## ESR OTT

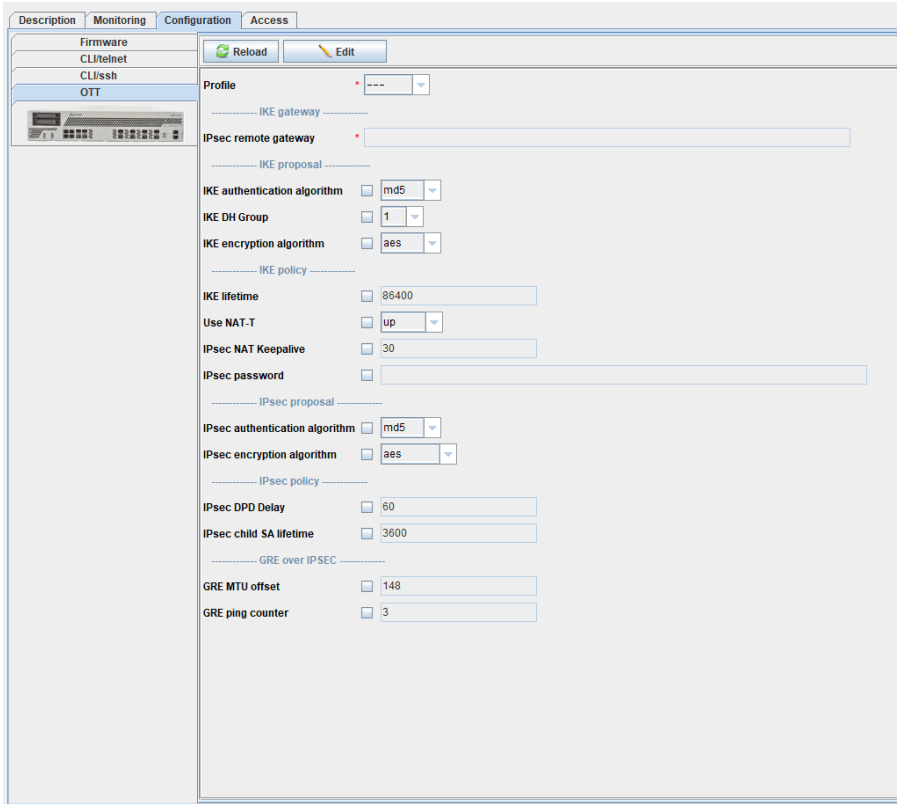
OTT parameter activation: in the *Access* tab, select the option *ServiceProvider* and enable BRAS by setting the checkbox *BRAS service* for ESR devices connected via OTT.



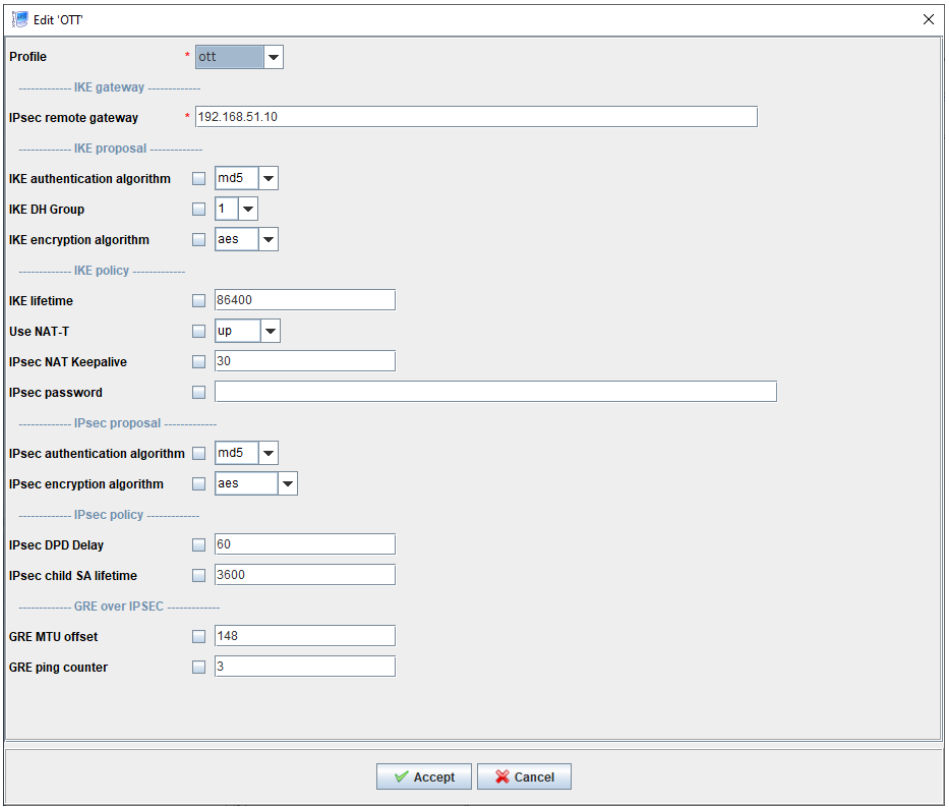

Set ESR parameters on ESR. To do this, create an OTT profile and a link to ESR.
To create an OTT profile, open the tab *OTT profiles* in *Wireless/AP initialization rule manager*. Create a profile with required parameters by clicking Add .




After the profile has been created, it can be linked to ESR. To do this, select ESR in the EMS tree and select the tab OTT in Configuration.

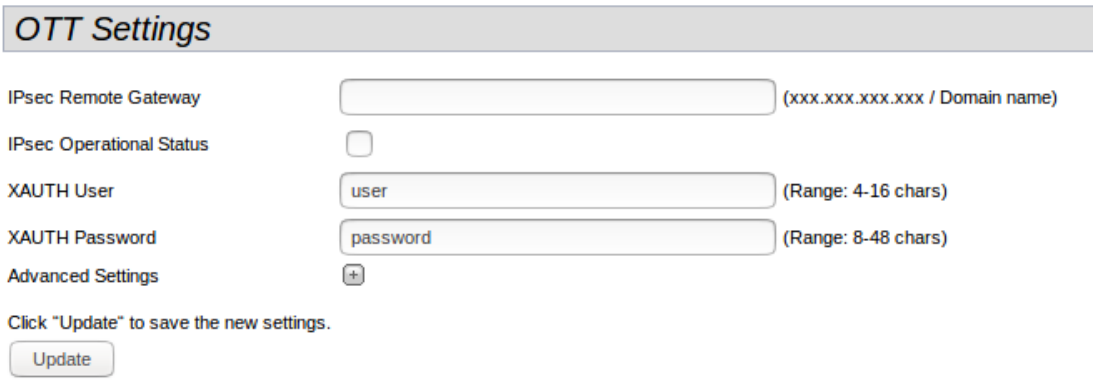



Open the OTT edit window by clicking Edit. Select the OTT profile created before and specify ESR public IP address. Specify the address of the gateway that the access point will request to as IPsec remote gateway. OTT profile parameters should match the parameters of OTT on ESR.




Configuring IPsec on AP without the Service Activator

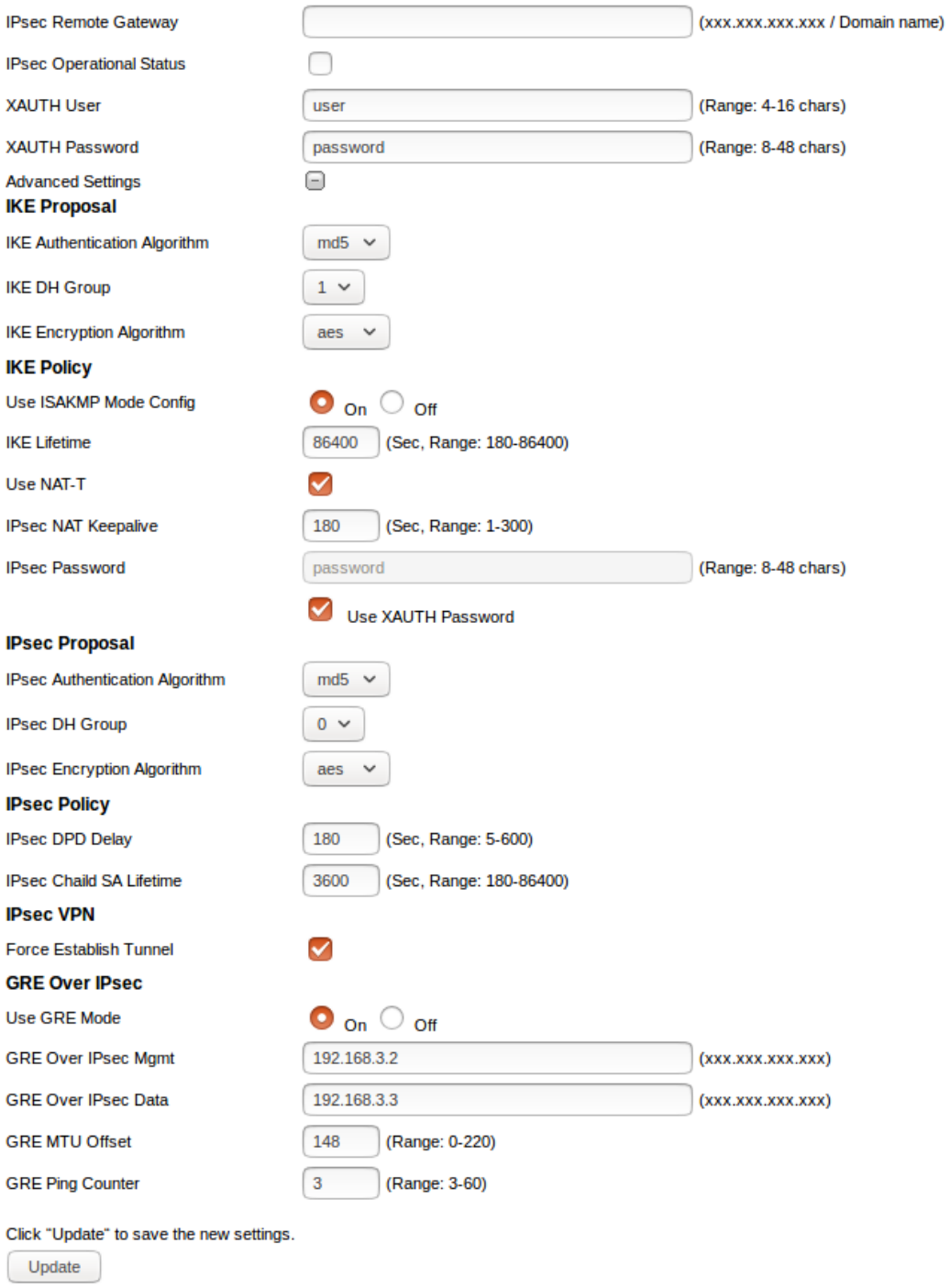
Open the menu Manage/OTT settings in the WEB interface of the access point



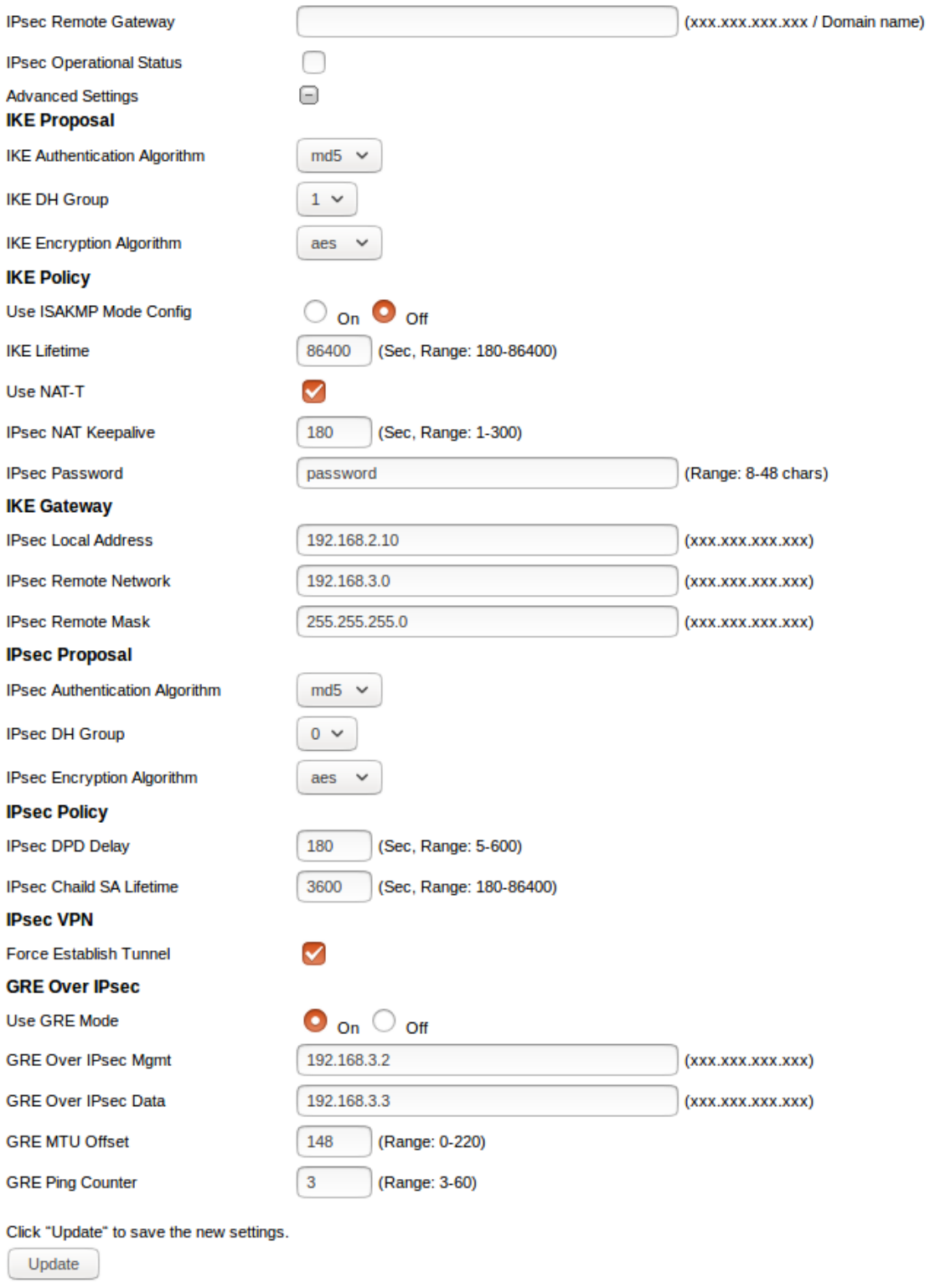

In brief menu, it will be sufficient to specify the address of a remote router with IPsec, XAUTH login and password (if passwords for XAUTH and IPsec are equal).

ⓘ If the checkbox Use XAUTH Password is enabled in Advanced Settings, XAUTH coincides with IPsec password. Otherwise, IPsec Password should be specified.

Extended IPsec parameters can be specified in Advanced Settings.




If the parameter Use ISAKMP Mode Config is set to On, the parameters GRE Over IPsec Mgmt and GRE Over IPsec Data are not taken into consideration. If the parameter Use ISAKMP Mode Config is set to Off, specify the parameters IKE Gateway, GRE Over IPsec Mgmt and GRE Over IPsec Data.




More about the parameters:

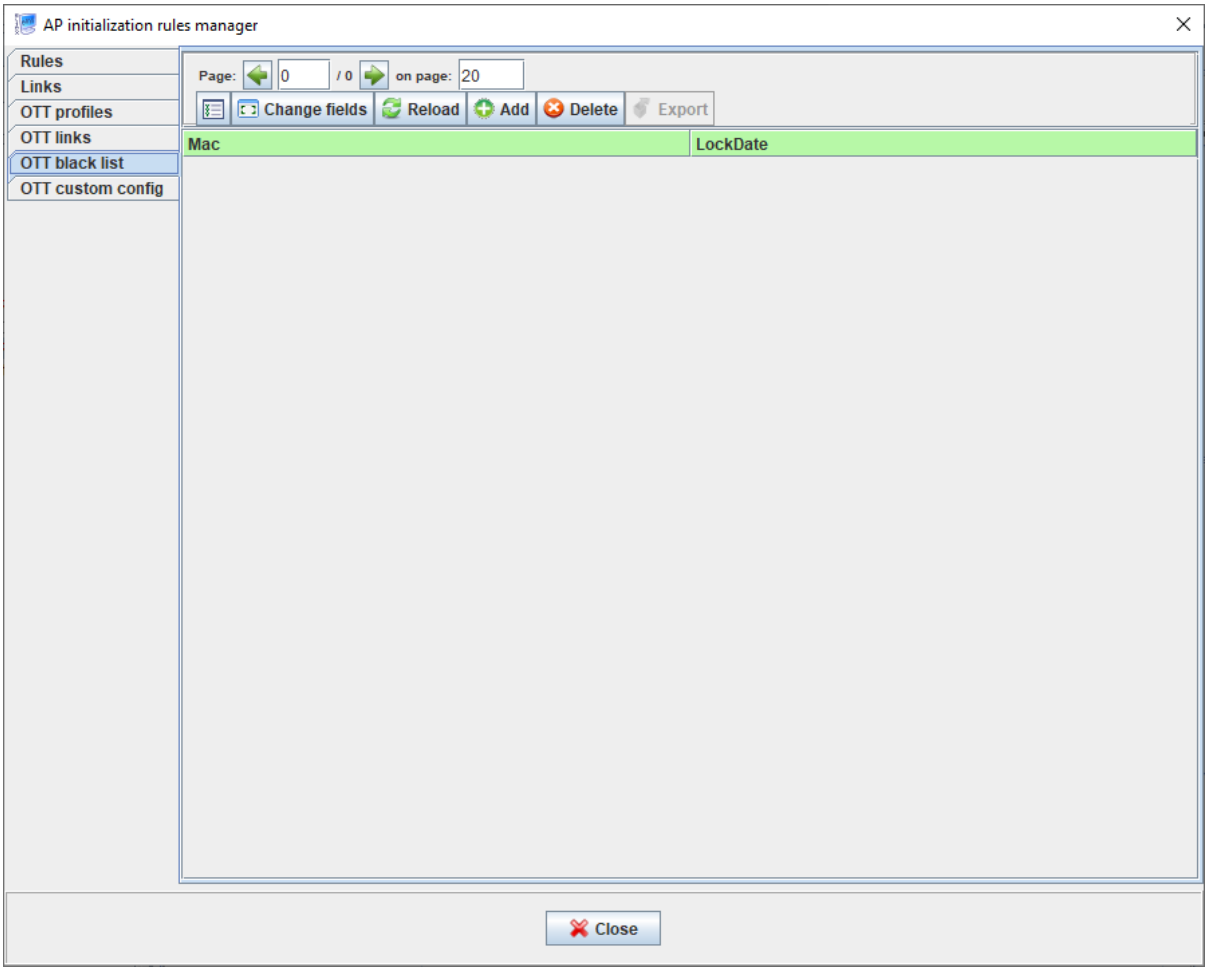
- **IPsec Remote Gateway –** Gateway IP address or domain name (xxx.xxx.xxx.xxx / Domain name).

- **IPsec Operational Status –** enabling IPsec.
- **XAUTH User –** name of XAUTH user, available if "Use ISAKMP Mode Config" is set to On (Range: 4-16 chars).
- **XAUTH Password –** password of XAUTH user, available if "Use ISAKMP Mode Config" is set to On (Range: 4-16 chars).
- **IKE Authentication Algorithm –** hashing algorithms to check data integrity (md5, sha1).
- **IKE DH Group –**group of Diffie-Hellman algorithms for establishing a shared secret key over an insecure channel (1, 2, 5).
- **IKE Encryption Algorithm –** encryption algorithm for Phase 1 of IPsec connection (AES128, DES, 3DES).
- **Use ISAKMP Mode Config –** if the parameter is set to «On» – ignore «GRE Over IPsec Mgmt», «GRE Over IPsec Data», «IPsec Local Address», «IPsec Remote Network», «IPsec Remote Mask».
- **IKE Lifetime –** IKE SA (Phase 1 lifetime) before reauthentication. Should be the same for both ends of IKE/IPsec tunnel (Sec, Range): 180–86400).
- **Use NAT-T –** enable this checkbox if a client is behind the NAT.
- **IPsec NAT Keepalive –** time between NAT keepalive packets (Sec, Range: 1-300).
- **IPsec Password –** shared password for IKE/ISPEC connection (Range: 8-48 chars).
- **IPsec Local Address –** client address used as a local IKE network with subnet mask 255.255.255.255 (/ 32). The value is ignored if "Use ISAKMP Mode Config" is set to On (xxx.xxx.xxx.xxx).
- **IPsec Remote Network –** remote IKE network. The value is ignored if "Use ISAKMP Mode Config" is set to On (xxx.xxx.xxx.xxx).
- **IPsec Remote Mask –** remote IKE subnet mask. The value is ignored if "Use ISAKMP Mode Config" is set to On (xxx.xxx.xxx.xxx).
- **Ipsec Authentication Algorithm –** hashing algorithms to check data integrity (md5, sha1).
- **IPsec DH Group –** Diffie-Hellman algorithms generate a shared secret key over an insecure channel. Value 0 allows using the secret key from IKE (0, 1, 2, 5)**.**
- **IPsec Encryption Algorithm –** encryption algorithm for Phase 1 of IPsec connection (AES128, DES, 3DES).
- **IPsec DPD Delay –** time interval after which ESR will send packages to the access point to check its accessibility (range: 5-600)
- **IPsec Child SA Lifetime –** IPsec VPN SA lifetime (Phase 2 lifetime) before reauthentication. Should be the same for both ends of IKE/IPsec tunnel. The value should be less than IKE Lifetime (Sec, Range: 180-86400).
- **IPsec Child SA Lifetime –** enable or disable GRE via IPsec. Is necessary because GRE local IP address uses IPsec local IP address.
- **GRE Over IPsec Mgmt –** GRE remote IP address for the Management tunnel (xxx.xxx.xxx.xxx).
- **GRE Over IPsec Data –** GRE remote IP address for the Management tunnel (xxx.xxx.xxx.xxx).
- **GRE MTU Offset –** device MTU. Calculated as MTU standard value - GRE MTU Offset.
- **GRE Ping Counter –** the number of gre-management-ip pings. If no response is sent, an IPsec connection will be re-established. gre-management-ip is pinged every 10 seconds. The parameter takes values from 3 to 60. Default value is 3.

IPsec child SA lifetime value should be less than IKE lifetime value. Moreover, IKE lifetime should be a multiple of IPsec child SA lifetime. By default, IKE lifetime is set to 86400 (24 hours), and IPsec child SA lifetime is set to 3600 (an hour). Consequently, IPsec key will be changed 24 times per day, and IKE — one time.

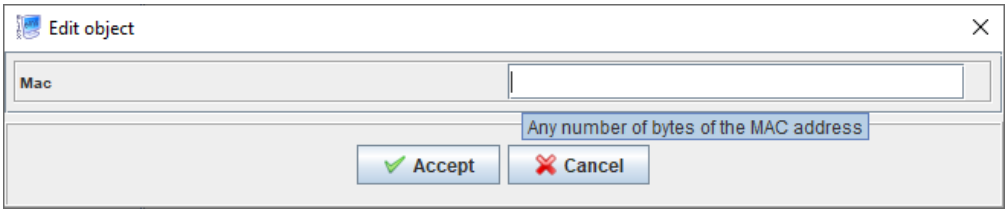
## OTT black list

OTT black list management can be carried out via GUI EMS.
Open Wireless/AP initialization rules manager/OTT black list




Click 

, and a window for MAC address entering will be opened. Enter MAC address of an AP to add it to the black list.




MAC address may contain any number of bytes. All MAC addresses that have the same beginning will be banned.
For example, if the string aa:bb:01 has been added to the black list, the addition of aa:bb:01:02:03:04 will

be rejected with a message: "aa:bb:01 has been already added to the black list". If an access point has been added to the black list, it will not get into the "sandbox".

### Deleting OTT link

Conditions under which OTT links are deleted:

- when an AP initialization link is deleted, an OTT link is deleted in EMS
- when an AP is replaced, an OTT link is deleted in EMS. It can be established again if necessary
- when ESR is deleted from EMS, all its OTT links are deleted too
- when ESR IP is changed in EMS, all its OTT links are deleted
- when ESR is deleted from EMS, its OTT station is deleted
- when ESR is put into another domain, all its OTT links should be deleted

Checking if an OTT station has been deleted:

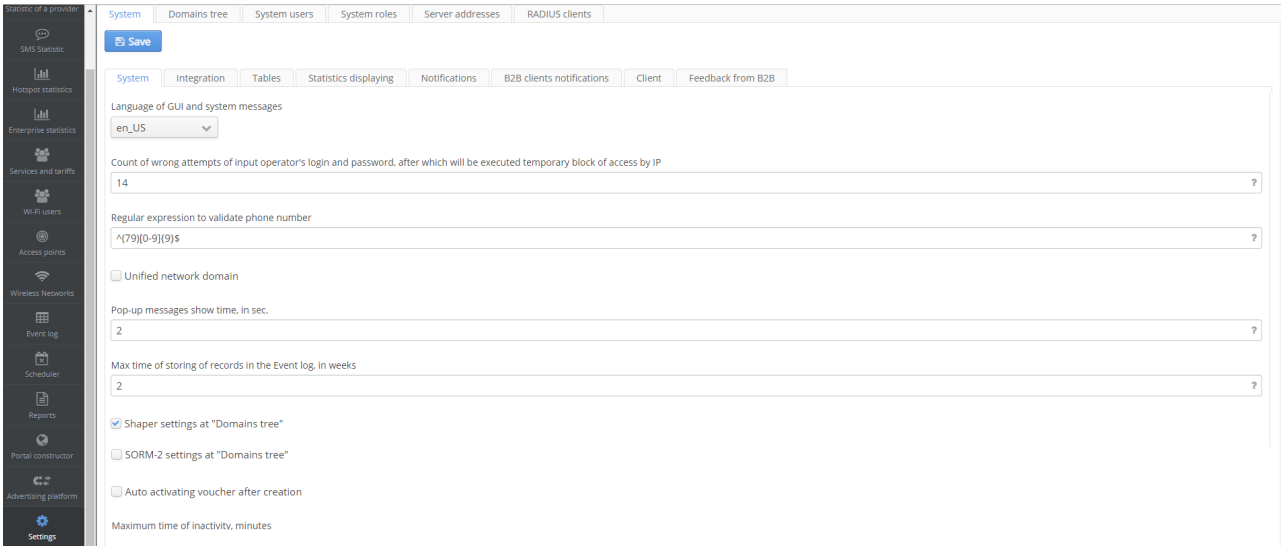
```
$ mongo
> use ott;
> db.station.find({esr_ip: '<esr ip address>'}).pretty();
```

Checking if OTT links were deleted:

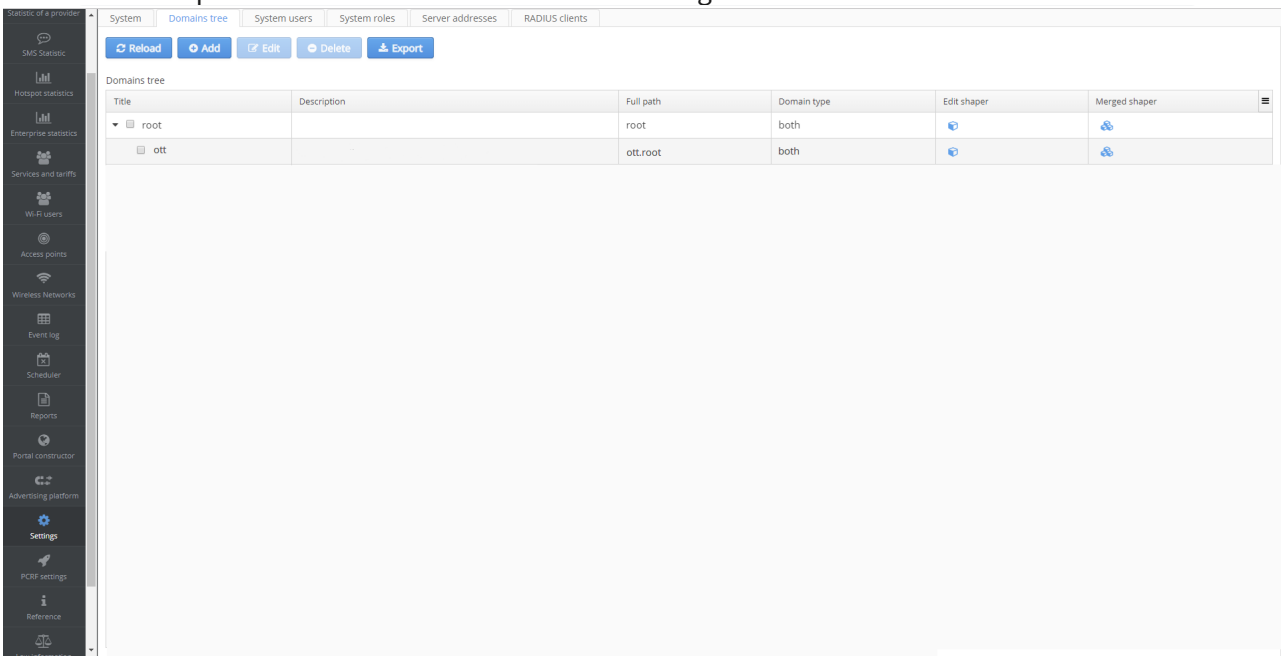
```
$ mongo
> use ott;
> db.xauth.find({esr_ip: '<esr ip address>'}).pretty();
> db.xauth.find({mac: '<AP mac address>'}).pretty();
```

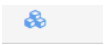
### Shaper settings via the Admin Panel

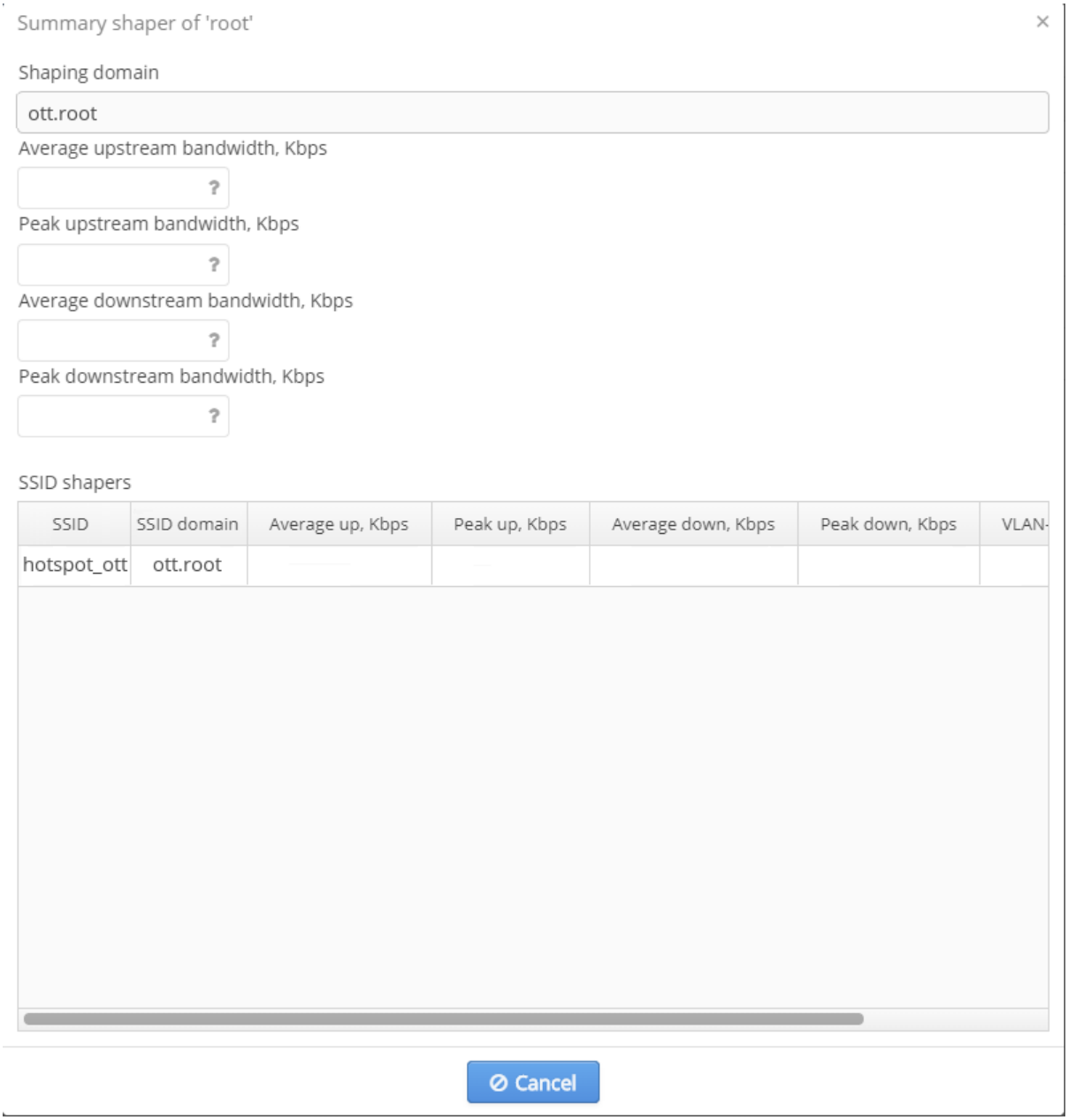
In the Admin Panel, in the "System" tab of Settings menu, enable the checkbox "Shaper settings at Domains tree", exit the Admin Panel and enter it again.




Enable SSID shaper in the "Domain tree" tab of the Settings menu.




Click the button  in the column "Merged shaper" and set the shaper parameters on SSID in the opened window.




## NBI for OTT management

To work with OTT a number of commands was created in NBI.
Relevant command documentation can be found in eltex-radius-nbi package. It becomes accessible after the package is downloaded via http://localhost:8080/eltex-radius-nbi/asciidoc/
Follow this link to get the WDSL file: http://localhost:8080/axis2/services/RadiusNbiService?wsdl
(replace localhost with the IP address of a server with NBI)

## Annex 1. List of IPsec parameters in the OTT profile

```
Description IKE authentication algorithm (md5, sha1), md5 by default
Name ipsec.auth-alg
Regex (md5|sha1)

Description IKE DH Group (1, 2, 5), 1 by default
Name ipsec.dh-group
Regex (1|2|5)

Description IPSEC DPD Delay (5..600), 60 by default
Name ipsec.dpd-delay
Regex ([5-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|[2-5][0-9][0-9]|600)

Description IKE encryption algorithm (aes, des, 3des), aes by default
Name ipsec.encrypt-alg
Regex (aes|des|3des)

Description Force establish tunnel (UP, DOWN), UP by default
Name ipsec.force-establish
Regex (UP|DOWN)

Description Use GRE mode (UP, DOWN), UP by default
Name ipsec.gre-mode
Regex (UP|DOWN)

Description GRE mtu offset (0..220), 148 by default
Name ipsec.gre-mtu-offset
Regex ([0-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|220|2[0-1][0-9])

Description IKE lifetime (180..86400), 86400 by default
Name ipsec.lifetime
Regex (18[0-9]|19[0-9]|[2-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|1000[0-9]|100[1-9][0-9]|10[1-9][0-9]
[0-9]|1[1-9][0-9][0-9][0-9]|[2-7][0-9][0-9][0-9][0-9]|86400|86[0-3][0-9][0-9]|8[0-5][0-9][0-9][0-9]
)

Description Use ISAKMP mode config (UP, DOWN), UP by default
Name ipsec.mode-cfg
Regex (UP|DOWN)

Description Use NAT-T (UP, DOWN), UP by default
Name ipsec.nat
Regex (UP|DOWN)

Description IPSEC NAT Keepalive (1..300), 30 by default
Name ipsec.nat-keepalive
Regex ([1-9]|[1-9][0-9]|10[0-9]|1[1-9][0-9]|2[0-9][0-9]|300)
```

```
Description IPSEC password (8-48 chars)
Name ipsec.password
Regex ([A-Za-z0-9]{8,48})

Description IPSEC DH Group (0, 1, 2, 5), 0 by default
Name ipsec.pfs-group
Regex (0|1|2|5)

Description IPSEC authentication algorithm (md5, sha1), md5 by default
Name ipsec.sa-auth-alg
Regex (md5|sha1)

Description IPSEC encryption algorithm (aes, des, 3des), aes by default
Name ipsec.sa-encrypt-alg
Regex (aes|des|3des)

Description IPSEC child SA lifetime (180..86400), 3600 by default
Name ipsec.sa-lifetime
Regex (18[0-9]|19[0-9]|[2-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|1000[0-9]|100[1-9][0-9]|10[1-9][0-9]
[0-9]|1[1-9][0-9][0-9][0-9]|[2-7][0-9][0-9][0-9][0-9]|86400|86[0-3][0-9][0-9]|8[0-5][0-9][0-9][0-9]
)

Description IPSEC operational status (UP, DOWN), UP by default
Name ipsec.status
Regex (UP|DOWN)

Description Use XAUTH password as IPSEC password (on/off) default off
Name ipsec.use-xauth-passwd
Regex (on|off)

Description XAUTH password (8-48 chars)
Name ipsec.xauth-password
Regex ([A-Za-z0-9]{8,48})

Description XAUTH user (4-16 chars)
Name ipsec.xauth-user
Regex ([A-Za-z0-9]{4,16})

Description IPSEC remote gateway (IP or URL)
Name ipsec.remote-gateway
<ax273:valueRegex xsi:nil="true"/>
```

## Annex 2. Description of errors returned by the Service Activator to access points

| **Message** | |
|---|---|
| Connection refused | The Service Activator is not installed, or port 8042 is blocked |
| "code":4022, "msg":"No init link found" | No initialization rule links to the AP |

| | |
|---|---|
| "code":1,"msg":"In request by key 'domain' value is empty or null" | There are no ESR devices with OTT enabled (OTT checkbox in the tab "Access") in the domain specified in the initialization rule link |
| "code":4024, "msg":"No OTT station configured" | There are no ESR profiles with OTT profile linked to IP address of ESR device with OTT enabled, or such ESR devices are unavailable. |
| "code":4023 | NB communication error |
| "code": 4025, "msg": "/ott/upgrade/WOP-12ac-LR-RevB.tar.gz" | AP firmware is not relevant. Update is required |

## Annex 3. ESR configuration example

Examples of ESR configuration on a test bench.

**Example 1**

The example is for the version 1.6.2 with BGP for ESR models without EoGRE tunnel support. The following addressing is used in the example:

1) gi1/0/1.4092: 10.12.20.4/28 - address directed to the Internet for IPsec termination;
2) gi1/0/1.212: 100.64.0.66/30 - seam address directed to VRF backbone for connection to SoftWLC, DHCP and DNS servers;
3) gi1/0/1.213: 100.64.0.70/30 - seam address directed to VRF nat for clients to access the Internet;
4) bridge 1: 192.168.200.49/28 и 192.168.200.50/28 - addresses to terminate EoGRE from access points for management and client traffic tunnels respectively;
5) bridge 3: 192.168.128.0/22 - subnetwork for AP management addresses. 192.168.128.1 is used as an address for managing ESR from SoftWLC;
6) bridge 10: 198.18.160.0/22 - subnetwork for AP clients. Default gateway for clients - 198.18.160.1, DNS 100.123.0.2;
7) 172.31.252.0/22 - subnetwork for addresses, assigned to access points via mode config and used to establish EoGRE on AP side;
8) 100.110.123.0/24 - management subnetwork. 100.123.0.2 - SoftWLC address, DHCP, DNS.

As the default gateway is directed to the Internet connection via gi1/0/1.4092, PBR rule named "users_map" in ESR configuration is used to direct client traffic via the interface gi1/0/1.213.

**Конфигурация**

```
hostname esr-ipsec

object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ipsec_ports
  port-range 500
  port-range 4500
exit
object-group service dns
  port-range 53
exit

object-group network SoftWLC
  ip prefix 100.123.0.0/24
exit
object-group network ipsec_remote_address
  ip prefix 10.100.0.0/16
  ip prefix 172.31.252.0/22
exit
object-group network gre_termination
  ip prefix 192.168.200.48/28
exit
object-group network AP_mgmt
  ip prefix 192.168.128.0/22
  ip prefix 198.18.160.0/22
exit
object-group network AP_users
  ip prefix 198.18.160.0/22
exit

syslog console none

radius-server timeout 10
radius-server retransmit 5
radius-server host 100.123.0.2
  key ascii-text encrypted 88B11079B9014FAAF7B9
  timeout 11
  priority 20
  source-address 192.168.128.1
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
```

```
aaa radius-profile PCRF
  radius-server host 100.123.0.2
exit
das-server COA
  key ascii-text encrypted 88B11079B9014FAAF7B9
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

tech-support login enable
root login enable

vlan 3
  force-up
exit
vlan 10
  force-up
exit

security zone trusted
exit
security zone untrusted
exit
security zone ipsec
exit
security zone gre
exit
security zone users
exit

ip access-list extended users_pbr
  rule 10
    action deny
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 11
    action deny
    match protocol udp
    match destination-port 53
    enable
  exit
  rule 20
    action permit
    enable
  exit
```

```
exit

route-map out_BGP_AP
  rule 10
    match ip address object-group AP_mgmt
    action permit
  exit
exit
route-map out_BGP_NAT
  rule 10
    match ip address object-group AP_users
    action permit
  exit
exit
route-map users_map
  rule 10
    match ip access-group users_pbr
    action set ip next-hop verify-availability 100.64.0.69 10
    action permit
  exit
exit
router bgp 64604
  address-family ipv4
    router-id 198.18.156.1
    redistribute connected
    neighbor 100.64.0.65
      remote-as 12389
      route-map out_BGP_AP out
      update-source 100.64.0.66
      enable
    exit
    neighbor 100.64.0.69
      remote-as 12389
      route-map out_BGP_NAT out
      update-source 100.64.0.70
      enable
    exit
    enable
  exit
exit

snmp-server
snmp-server system-shutdown
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 100.123.0.2
exit

snmp-server enable traps
snmp-server enable traps config
```

```
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment fan
snmp-server enable traps environment fan-speed-changed
snmp-server enable traps environment fan-speed-high
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps environment board-overheat-temp
snmp-server enable traps environment board-supercooling-temp
snmp-server enable traps wifi
snmp-server enable traps wifi wifi-tunnels-number-in-bridge-high
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
```

```
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon fan
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
  description "gre_termination"
  vlan 1
  security-zone gre
  ip address 192.168.200.49/28
  ip address 192.168.200.50/28
  enable
exit
bridge 3
  description "AP_mgmt"
  vlan 3
  security-zone trusted
  ip address 192.168.128.1/22
  ip helper-address 100.123.0.2
  ip tcp adjust-mss 1312
  enable
exit
bridge 10
  description "Users"
  vlan 10
  security-zone users
  ip address 198.18.160.1/22
  ip helper-address 100.123.0.2
  ip policy route-map users_map
  ip tcp adjust-mss 1312
  location data10
  enable
exit

interface gigabitethernet 1/0/1
```

```
  description "UpLink"
exit
interface gigabitethernet 1/0/1.212
  description "VRF_backbone"
  security-zone trusted
  ip address 100.64.0.66/30
  ip tcp adjust-mss 1312
exit
interface gigabitethernet 1/0/1.213
  description "VRF_nat"
  security-zone untrusted
  ip address 100.64.0.70/30
  ip tcp adjust-mss 1312
exit
interface gigabitethernet 1/0/1.1000
  description "adm_net"
  security-zone trusted
  ip address 100.110.0.133/23
exit
interface gigabitethernet 1/0/1.4092
  description "IPsec"
  security-zone ipsec
  ip address 10.12.20.4/28
exit
tunnel softgre 1
  description "mgmt"
  mode management
  local address 192.168.200.49
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 3
  enable
exit
tunnel softgre 2
  description "data"
  mode data
  local address 192.168.200.50
  default-profile
  enable
exit

security zone-pair trusted self
  rule 10
    action permit
    enable
  exit
exit
security zone-pair users self
  rule 10
```

```
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
exit
security zone-pair users untrusted
  rule 10
    action permit
    enable
  exit
exit
security zone-pair users trusted
  rule 10
    action permit
    match protocol udp
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol udp
    match destination-port dns
    enable
  exit
exit
security zone-pair ipsec self
  rule 1
    action permit
    match protocol udp
    match destination-port ipsec_ports
    enable
  exit
  rule 2
    action permit
    match protocol esp
    enable
  exit
  rule 3
    action permit
    match protocol gre
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
  rule 4
    action permit
    match protocol icmp
    enable
```

```
  exit
exit
security zone-pair trusted trusted
  rule 10
    action permit
    enable
  exit
exit

address-assignment pool ipsec_xauth_pool
  ip prefix 172.31.252.0/22
  data-tunnel address 192.168.200.50
  management-tunnel address 192.168.200.49
exit

security ike proposal dh1_md5_aes128
  authentication algorithm md5
  encryption algorithm aes128
exit

security ike policy psk_xauth
  lifetime seconds 86400
  pre-shared-key ascii-text testing123
  authentication method xauth-psk-key
  authentication mode radius
  proposal dh1_md5_aes128
exit

security ike gateway xauth_gw
  ike-policy psk_xauth
  local address 10.12.20.4
  local network 192.168.200.48/28
  remote address any
  remote network dynamic pool ipsec_xauth_pool
  mode policy-based
  dead-peer-detection action clear
  dead-peer-detection interval 60
  dead-peer-detection timeout 180
exit

security ipsec proposal md5_aes128_esp
  authentication algorithm md5
  encryption algorithm aes128
exit

security ipsec policy ipsec_pol
  proposal md5_aes128_esp
exit

security ipsec vpn xauth_ipsec
  mode ike
```

```
  ike establish-tunnel by-request
  ike gateway xauth_gw
  ike ipsec-policy ipsec_pol
  enable
exit

security passwords history 0
ip dhcp-relay

ip route 0.0.0.0/0 10.12.20.2

wireless-controller
  nas-ip-address 192.168.128.1
  resp-time 3
  failure-count 3
  data-tunnel configuration radius
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit
```

**Example 2**
The example given is for the version 1.4.0 with static routing (for ESR models without EoGRE tunnel support). The following addressing is used in the example:
1) bridge 1: 192.168.171/24 - address directed to the Internet and used for IPsec termination;
2) bridge 2: 192.168.110.0.37/24 - administrative subnetwork, the address is used for administrator access;
2) bridge 3: 101.0.0.171/24 - seam address to connect to SoftWLC, DHCP and DNS servers. Is used as a management address from SoftWLC side. SoftWLC address 101.0.0.24;
3) bridge 5: 192.168.7.1/30 and 192.168.7.2.30 - EoGRE termination address from AP, for management tunnels and client traffic respectively;
4) bridge 6: 172.31.239.1/26 - subnetwork for AP management addresses;
5) bridge 7: 172.31.239.65/26 - subnetwork for AP clients;
6) bridge 94: 10.12.12.1/30 - seam address to provide clients with Internet access;
7) 172.31.250.0/24 - subnetwork for addresses, assigned to access points via mode config and used to establish EoGRE on AP side;
As the default gateway is directed to the side of Internet connection via bridge 1, PBR rule named "clients_br7" in ESR configuration is used to direct client traffic via bridge 94.

**Конфигурация**

```
hostname esr-ipsec

tech-support login enable
root login enable

syslog max-files 3
syslog file-size 512

object-group service telnet
  port-range 23
exit
object-group service ssh
  port-range 22
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ntp
  port-range 123
exit
object-group service ipsec_ports
  port-range 500
  port-range 4500
exit
object-group service snmp
  port-range 161-162
exit
object-group service COA
  port-range 3799
  port-range 31812-31813
  port-range 1812-1813
exit
object-group service redirect
  port-range 3128
  port-range 3129
exit

object-group network SoftWLC
  ip address-range 101.0.0.24
exit
object-group network ipsec_remote_address
  ip prefix 172.31.250.0/24
exit
object-group network gre_termination
  ip prefix 192.168.7.0/30
```

```
exit

object-group url defaultserv
  url http://eltex-co.ru
exit

#Configuring interaction with the RADIUS server for access points' data tunnel dynamic
management.
radius-server timeout 10
radius-server retransmit 5
radius-server host 101.0.0.24
  key ascii-text testing123
  timeout 11
  priority 20
  source-address 101.0.0.171
  auth-port 31812
  acct-port 31813
  retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
  radius-server host 101.0.0.24
exit

#Configuring ESR for the RADIUS server to communicate with it.
das-server COA
  key ascii-text testing123
  port 3799
  clients object-group SoftWLC
exit
aaa das-profile COA
  das-server COA
exit

vlan 2
  force-up
exit
vlan 7
  name "mgmt"
  force-up
exit
vlan 100
  name "user"
  force-up
exit
vlan 808
  name "GRE"
  force-up
exit
vlan 1001
  name "from_SoftWLC"
```

```
  force-up
exit
vlan 1108
  force-up
exit
vlan 4094
  force-up
exit

security zone trusted
exit
security zone user
exit
security zone mgmt
exit
security zone gre
exit
security zone ipsec
exit
security zone clients_inet
exit

#Configuring the subnetwork with client addresses that will be transferred to another router
using policy-based routing.
ip access-list extended users_filter
  rule 1
    action permit
    match protocol any
    match source-address 172.31.239.64 255.255.255.192
    match destination-address any
    enable
  exit
exit

#DHCP request for client addresses extension should be passed to a DHCP server that has the same
IP as SoftWLC.
ip access-list extended clients_dhcp
  rule 1
    action permit
    match protocol udp
    match source-address 172.31.239.64 255.255.255.192
    match destination-address 101.0.0.24 255.255.255.255
    match source-port 68
    match destination-port 67
    enable
  exit
exit

#Configuring route-map, specifying routers to which client traffic will be transferred.
route-map clients_br7
  rule 1 #Pass clients' DHCP request to the DHCP server.
```

```
    match ip access-group clients_dhcp
    action set ip next-hop verify-availability 101.0.0.24 10
    action permit
  exit
  rule 2 #Pass other traffic to a router used to provide client with Internet access.
    match ip access-group users_filter
    action set ip next-hop verify-availability 10.12.12.2 10
    action permit
  exit
exit

snmp-server
snmp-server system-shutdown #Permit ESR reset by running EMS SNMP command.
snmp-server community "private1" rw
snmp-server community "public11" ro

snmp-server host 101.0.0.24
exit

#The interface for the Internet terminates IPsec connections of access points.
bridge 1
  vlan 1108
  security-zone ipsec
  ip address 192.168.108.171/24
  enable
exit

#The interface of administrative management subnetwork is optional.
bridge 2
  vlan 2
  security-zone trusted
  ip address 192.168.110.37/24
  enable
exit

#The interface for interaction with SoftWLC.
bridge 3
  description "SoftWLC"
  vlan 1001
  security-zone mgmt
  ip address 101.0.0.171/24
  enable
exit

#The interface to terminate AP GRE connections.
bridge 5
  vlan 808
  security-zone gre
  ip address 192.168.7.1/30
  ip address 192.168.7.2/30
  enable
```

```
exit

#The interface for AP management.
bridge 6
  vlan 7
  security-zone mgmt
  ip address 172.31.239.1/26
  ip helper-address 101.0.0.24
  ip tcp adjust-mss 1312
  protected-ports
  protected-ports exclude vlan
  enable
exit

#The interface for AP clients.
bridge 7
  vlan 100
  security-zone user
  ip address 172.31.239.65/26
  ip helper-address 101.0.0.24
  ip policy route-map clients_br7 #Enabling policy-based routing on the interface.
  ip tcp adjust-mss 1312
  location testing2
  protected-ports
  protected-ports exclude vlan
  enable
exit

#The interface to access the router where AP clients' traffic will be directed to.
bridge 94
  vlan 4094
  security-zone clients_inet
  ip address 10.12.12.1/30
  ip tcp adjust-mss 1312
  enable
exit

interface port-channel 1
  switchport forbidden default-vlan
  switchport general acceptable-frame-type tagged-only
  switchport general allowed vlan add 2,1001,1108,4094 tagged
exit
interface gigabitethernet 1/0/1
  channel-group 1 mode auto
exit
interface gigabitethernet 1/0/2
  channel-group 1 mode auto
exit
interface gigabitethernet 1/0/3
  shutdown
  security-zone trusted
```

```
  ip firewall disable
exit
interface gigabitethernet 1/0/4
  shutdown
  security-zone trusted
  ip firewall disable
exit
interface tengigabitethernet 1/0/1
  shutdown
  ip firewall disable
  switchport forbidden default-vlan
exit
interface tengigabitethernet 1/0/2
  shutdown
  ip firewall disable
  switchport forbidden default-vlan
exit
exit
tunnel softgre 1
  description "mgmt"
  mode management
  local address 192.168.7.1
  default-profile
  enable
exit
tunnel softgre 1.1
  bridge-group 6
  enable
exit
tunnel softgre 2
  description "data"
  mode data
  local address 192.168.7.2
  default-profile
  enable
exit

security zone-pair trusted self
  rule 1
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port ssh
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match source-address any
```

```
    match destination-address any
    match source-port any
    match destination-port telnet
    enable
  exit
  rule 3
    action permit
    match protocol icmp
    match source-address SoftWLC
    match destination-address any
    enable
  exit
exit
security zone-pair user self
  rule 10
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port redirect
    enable
  exit
exit
security zone-pair clients_inet self
  rule 10
    action permit
    match protocol any
    match source-address any
    match destination-address any
  exit
exit
security zone-pair user clients_inet
  rule 1
    action permit
    match protocol any
    match source-address any
    match destination-address any
    enable
  exit
exit
security zone-pair ipsec self
```

```
  rule 1
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port ipsec_ports
    match destination-port ipsec_ports
    enable
  exit
  rule 2
    action permit
    match protocol esp
    match source-address any
    match destination-address any
    enable
  exit
  rule 3 #As GRE traffic will be obtained from IPsec packets, it will be considered to come from
the same area as a parent packet.
    action permit
    match protocol gre
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
  rule 4
    action permit
    match protocol icmp
    match source-address ipsec_remote_address
    match destination-address gre_termination
    enable
  exit
exit
security zone-pair mgmt self
  rule 1
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port ssh
    enable
  exit
  rule 2
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port telnet
    enable
  exit
```

```
rule 3
  action permit
  match protocol icmp
  match source-address SoftWLC
  match destination-address any
  enable
exit
rule 4
  action permit
  match protocol udp
  match source-address SoftWLC
  match destination-address any
  match source-port any
  match destination-port snmp
  enable
exit
rule 5
  action permit
  match protocol udp
  match source-address SoftWLC
  match destination-address any
  match source-port any
  match destination-port COA
  enable
exit
rule 6
  action permit
  match protocol tcp
  match source-address SoftWLC
  match destination-address any
  match source-port any
  match destination-port COA
  enable
exit
rule 7
  action permit
  match protocol icmp
  match source-address any
  match destination-address any
  enable
exit
rule 10
  action permit
  match protocol udp
  match source-address any
  match destination-address any
  match source-port dhcp_client
  match destination-port dhcp_server
  enable
exit
rule 11
```

```
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
  exit
exit
security zone-pair mgmt mgmt
  rule 1
    action permit
    match protocol icmp
    match source-address any
    match destination-address any
    enable
  exit
  rule 10
    action permit
    match protocol udp
    match source-address any
    match destination-address any
    match source-port dhcp_client
    match destination-port dhcp_server
    enable
  exit
  rule 20
    action permit
    match protocol udp
    match source-address SoftWLC
    match destination-address any
    match source-port any
    match destination-port snmp
    enable
  exit
  rule 21
    action permit
    match protocol udp
    match source-address any
    match destination-address SoftWLC
    match source-port any
    match destination-port snmp
    enable
  exit
  rule 22
    action permit
    match protocol tcp
    match source-address SoftWLC
    match destination-address any
    match source-port any
    match destination-port snmp
```

```
    enable
  exit
  rule 23
    action permit
    match protocol tcp
    match source-address any
    match destination-address SoftWLC
    match source-port any
    match destination-port snmp
  exit
  rule 30
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port telnet
    enable
  exit
  rule 31
    action permit
    match protocol tcp
    match source-address any
    match destination-address any
    match source-port any
    match destination-port ssh
    enable
  exit
  rule 49
    action permit
    match protocol udp
    match source-address any
    match destination-address SoftWLC
    match source-port any
    match destination-port ntp
    enable
  exit
  rule 50
    action permit
    match protocol udp
    match source-address any
    match destination-address SoftWLC
    match source-port any
    match destination-port COA
    enable
  exit
exit
security zone-pair mgmt user
  rule 10
    action permit
    match protocol udp
```

```
    match source-address SoftWLC
    match destination-address any
    match source-port dhcp_server
    match destination-port dhcp_server
    enable
  exit
exit
security zone-pair gre ipsec
  rule 1
    action permit
    match protocol any
    match source-address gre_termination
    match destination-address ipsec_remote_address
    enable
  exit
exit

#Configuring the pool of addresses that will be assigned to access points via mode config.
address-assignment pool ipsec_pool_1
  ip prefix 172.31.250.0/24             #The pool of addresses that will be assigned to access
points
                                        #and used as a local IP (tunnel IP) for GRE tunnels.
                                        #Addresses should not overlap with other tunnel IP
addresses in EMS.
  data-tunnel address 192.168.7.2       #The address to which an AP will establish a GRE data
tunnel.
  management-tunnel address 192.168.7.1 #The address to which an AP will establish a GRE
management tunnel.
exit

#Configuring IKE proposal: MD5 hashing algorithm, Diffie-Hellman group DH1, AES128 encryption
algorithm.
security ike proposal dh1_md5_aes128
  authentication algorithm md5
  encryption algorithm aes128
exit

#Configuring IKE security policy.
security ike policy psk_xauth1
  lifetime seconds 86400               #Main connection lifetime (reauthorization will be carried
out upon expiry).
  pre-shared-key ascii-text testing123 #Password
  authentication method xauth-psk-key  #Enabling XAUTH extended authorization.
  authentication mode radius           #Using RADIUS server for extended authorization.
  proposal dh1_md5_aes128              #Using the proposal configured above.
exit

#Configuring gateways and subnetworks.
security ike gateway ike1_from_inet
  ike-policy psk_xauth1                    #Using the IKE policy configured above.
  local address 192.168.108.171            #The address for IPsec clients.
```

```
  local network 192.168.7.0/30             #The local subnetwork, traffic of which will be
encapsulated to IPsec packets.
  remote address any                       #The address of remote IPsec clients - permit
connections with any addresses.
  remote network dynamic pool ipsec_pool_1 #To assign parameters to a client, use the pool
configured above.
  mode policy-based                        #Using policy-based mode.
  dead-peer-detection action clear         #If an inaccessible IPsec client is detected, delete
his connection.
  dead-peer-detection interval 60          #The interval between dead-peer-detection packets.
  dead-peer-detection interval 180         #Time interval, upon expiry of which a remote IPsec
client will be considered as inaccessible,
                                           #if no response to DPD packets is received.
exit

#Configuring IPsec proposal: MD5 hashing algorithm, AES128 encryption algorithm, ESP protocol.
security ipsec proposal md5_aes128_esp
  authentication algorithm md5
  encryption algorithm aes128
exit

#Configuring IPsec policy.
security ipsec policy vpn1_pol1
  lifetime seconds 3600   #IPsec child SA lifetime (reauthorization will be carried out upon
expiry).
  proposal md5_aes128_esp #The IPsec proposal configured above.
exit

#Configuring IPsec VPN to which access point will connect.
security ipsec vpn for_INET_1
  mode ike                         #Using IKE.
  ike establish-tunnel by-request #IPsec connection is established upon request from the remote
endpoint.
  ike gateway ike1_from_inet       #Using gateway and subnetwork settings configured in IKE.
  ike ipsec-policy vpn1_pol1       #Using IPsec policy configured above.
  enable
exit

ip dhcp-relay

ip route 0.0.0.0/0 192.168.108.1 200

wireless-controller
  nas-ip-address 101.0.0.171
  data-tunnel configuration radius #Using dynamic data tunnel establishment
  aaa das-profile COA
  aaa radius-profile PCRF
  enable
exit
ip telnet server
```

```
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 101.0.0.24
  prefer
exit
```

If ESR 1200/1700 with version 1.4.1 or higher are used - configuration of a scheme with a loop through physical interfaces will be required to provide correct work of hardware EoGRE.

## Troubleshooting

### Service Activator logs

All Service Activator logs are keeped in the file **/var/log/eltex-wifi-sa/wifi-sa-server.log**. To obtain extended logs, set LogLevel = debug in the configuration file application.conf

### Viewing OTT information on access points

Run the following commands in AP CLI:

Viewing parameters of Service Activator's client part on an AP:
```
WEP-12ac_rev_C# get ipsec-activator
```

Viewing IPsec parameters received by an AP from the Service Activator:
```
WEP-12ac_rev_C# get ipsec-dynamic
```

Viewing URL of the Service Activator embedded in an AP:
```
WEP-12ac_rev_C# sh

/mnt/root # cd /etc/cert/
/etc/cert # cat sa-host.txt
https://126.0.10.4:8043
```

Viewing provider-id and MAC address of an AP in a certificate:
```
WEP-12ac_rev_C# sh

/etc/cert # openssl x509 -in /etc/cert/cert.pem -text -noout
WARNING: can't open config file: /etc/pki/tls/openssl.cnf
Certificate:
Data:
Version: 3 (0x2)
```

```
Serial Number:
e0:d9:e3:70:1d:00:bc:2a:aa:28:54:ee:9f:27:5a:77
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=OTT Certification Root (Test), O=Eltex Enterprise Ltd., OU=Wi-Fi,
C=RU, L=Novosibirsk
Validity
Not Before: Jan 1 00:00:00 1999 GMT
Not After : Jan 1 00:00:00 2100 GMT
Subject: CN=E0:D9:E3:70:1D:00, O=provider_eltex
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
........
```

where `e0:d9:e3:70:1d:00` - AP MAC address,
`provider_eltex` - Provider-ID

### Manual starting of the Service Activator's client part on an AP with debug enabled

*service-activator https://<Service Activator URL>:8043 --msg-type register --timeout 300 -C /etc/cert/cert.pem -K /etc/cert/key.pem -A /etc/cert/ca.pem -d 15*
Used to debug interaction of an AP with the Service Activator from an access point's side.

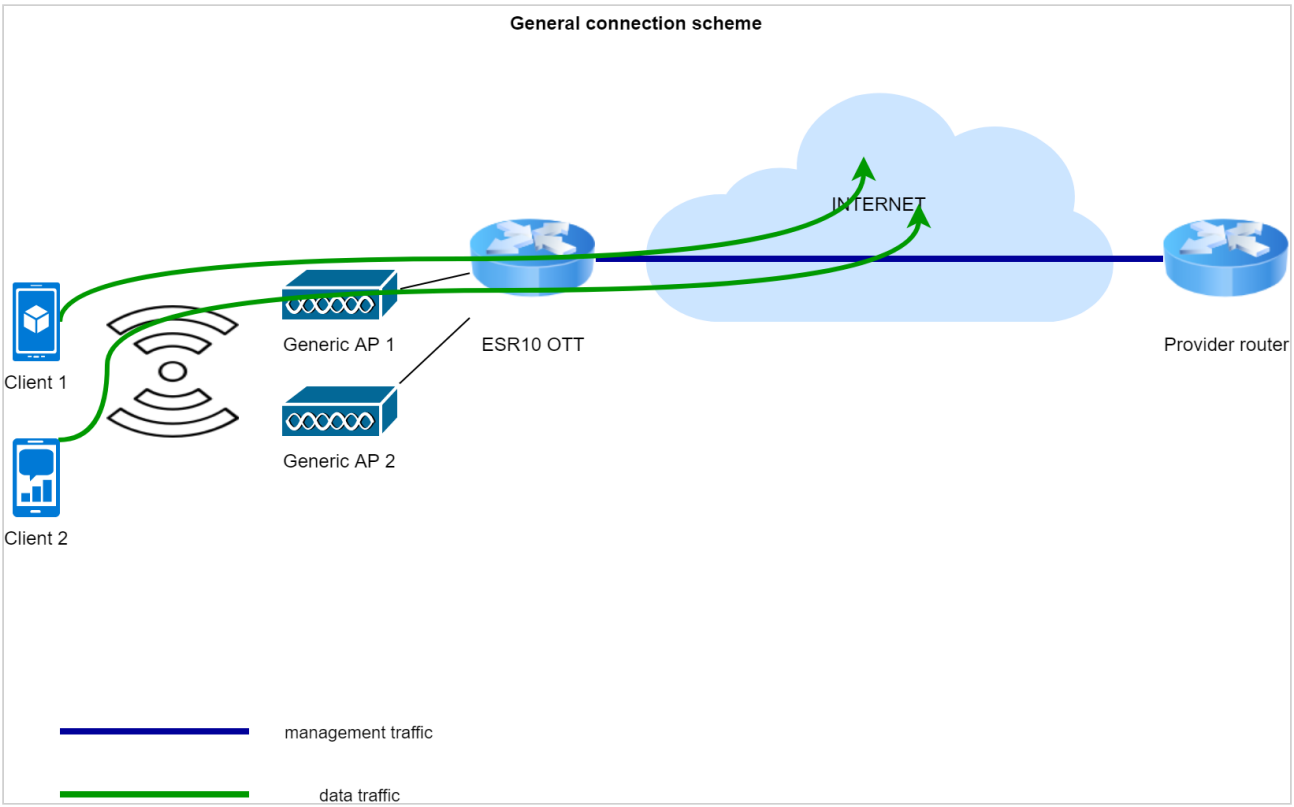
## v1.14_ESR-10+OTT+(1.6.0) Configuration and connection. General information (EN)


- General information
  - Requirements for connection points
  - Connection schemes
- Preconfiguration
  - Enabling the Service Activator client on ESR-10
  - ELTEX-WIFI-SA
  - ISC-DHCP-SERVER
- Configuring connection and initialization using a default rule
  - EMS
- Connecting clients
  - Configuring BRAS services and tariffs
  - Portal configuration
  - Configuring SSID
  - Creating L2 subnetworks

- Creating OTT custom configuration
- Creating a link for ESR-10 with OTT custom configuration
    - 1) A default OTT link was used for ESR-10, and it was put into the default domain
    - 2) Default OTT link is not used in EMS configuration, or MAC address of a device installed at a client's is known in advance.
- Appendices
    - Configuring OTT custom config, sent by the Service Activator
        - General description
        - Description of default configuration in the OTT custom config
        - Configuration for client connection
    - List of error codes sent by ESR-10 to the Service Activator


## General information

SoftWLC is supposed to be already configured for connecting AP OTT and working with BRAS (all the required services and tariffs are configured, interaction is provided), so their configuration is not given there.
To establish a GRE over IPsec tunnel, the same ESR as used for AP OTT tunnel establishment is applied. Additional setting is not required.
Connection scheme would provide clients with Internet access locally on the ESR-10 connection. Only a GRE over IPsec tunnel will be established to the root. This tunnel will be used for ESR-10 management and client redirection to the authorization portal.
To work with "OTT individual configuration" for ESR-10, the service "Jerry" should be installed. See more in v1.14_Jerry.

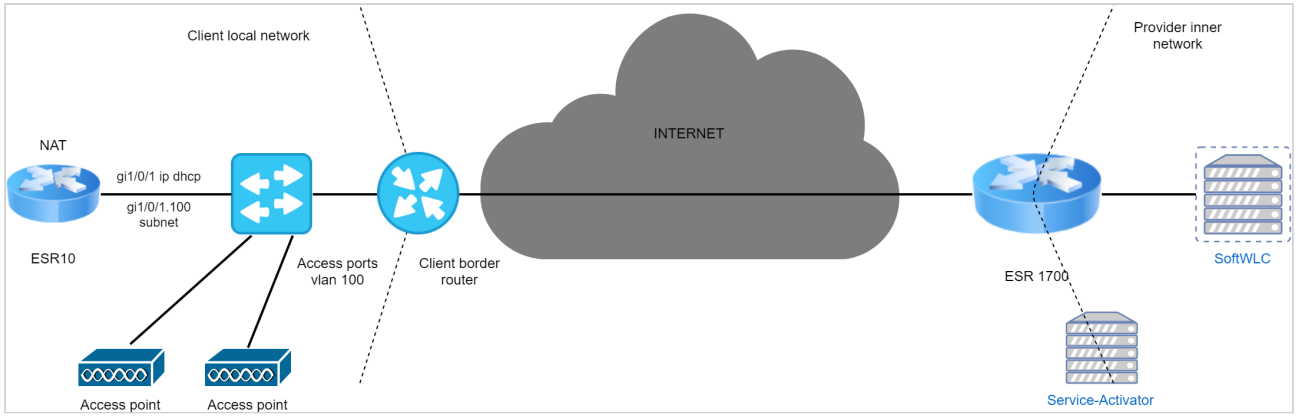


Requirements for connection points

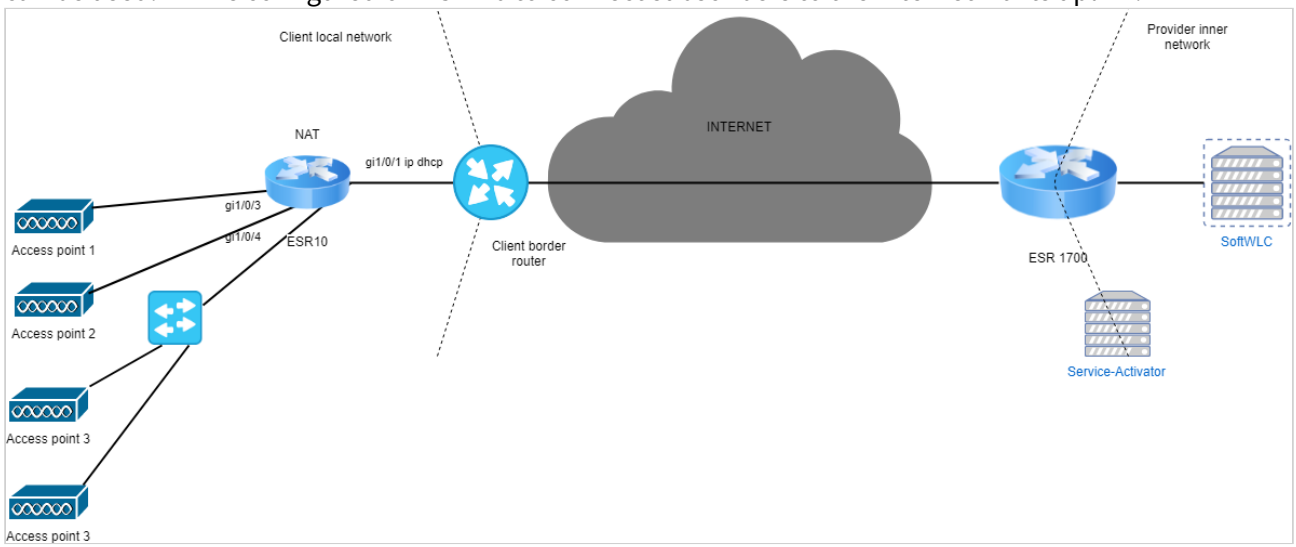
1) only the port gi1/0/1 ESR10 is used for Internet connection;
2) an address is assigned via DHCP. It should contain a default gateway and a DNS server
3) traffic that goes through ESR10 connection point to the Internet should be untagged.

Connection schemes

ESR-10 BRAS works at L3, which implies that clients will allways have a separate subnetwork with ESR-10 serving as a default gateway. Then client traffic can go to the Internet from ESR-10 primary address via NAT or via routing. In the second case, NAT provides a client's router with Internet access.
1. ESR-10 connects to the Internet via a client's router. Access points are connected to ESR-10 via a switch using a separate VLAN for SSID that terminates via a sub-interface on ESR-10 uplink and to which clients connect to. ESR-10 provides clients with Internet access using NAT.




2. ESR-10 is connected to a router that provides a client with Internet and is located at a client's network. Access points are connected directly to ESR-10 via a special port. If there are no available ports, a switch can be used. NAT is configured on ESR-10 to connect subscribers to the Internet via its uplink.



### Preconfiguration

Two ways of ESR-10 connection in the OTT mode are possible:
1) prior connection of ESR-10 and its initialization to a certain default domain by a default rule - in this case ESR-10 will be seen in the default domain, but it will not be used for the Internet access until it is put into the required client domain where a custom configuration agreed with a client will be assigned to it.
2) coordination with a client, creating an initialization rule link (with OTT custom configuration specified) by MAC address of ESR-10 that will be installed at a client's, adding all necessary settings to SoftWLC (L2 subnetworks, creating tariffs if needed). In this case, ESR-20 will get a required configuration right after its installation and will be ready to work.

#### Enabling the Service Activator client on ESR-10

OTT mode is not enabled on ESR-10 in the supply, so the device can be used as a standard router. If router configuration was changed - reset it to factory-config. Router with factory configuration will require to enter a password (enter "password"; when configuration from the Service Activator will be received, the password will be changed):

*esr-10(change-expired-password)# password password*

*esr-10(change-expired-password)# comm*

*Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.*

*2019-02-07T12:15:53+00:00 %CLI-I-CRIT: user admin from console  input: commit*

*esr-10(change-expired-password)# confirm*

*Configuration has been confirmed. Commit timer canceled.*

*2019-02-07T12:15:57+00:00 %CLI-I-CRIT: user admin from console  input: confirm*

*esr-10#*

To activate the mode, open debug and provide a link to the Service Activator:

*esr-10# debug*

*esr-10(debug)# service-activator url* https://sa.example.org:8043

After enabling the mode and receiving/updating the address via DHCP, the Service Activator client will be started and try to connect to the address specified in url.
To disable OTT, delete a line with the Service Activator URL using the command:

*esr-10(debug)# no service-activator url*

*esr-10(debug)# show service-activator url*

*esr-10(debug)#*

To change a link to access the Service Activator, provide a new one and restart ESR-10.

ELTEX-WIFI-SA

Add a current firmware to the directory /var/lib/eltex-wifi-sa/firmware/

```
root@softwlc-ott:/tftpboot# mv -v /tftpboot/esr1x-1.6.0-build3.firmware  /var/lib/eltex-wifi-sa/
firmware/

‘/tftpboot/esr1x-1.6.0-build3.firmware’ -> ‘ /var/lib/eltex-wifi-sa/firmware/esr1x-1.6.0-build3.firmware’
removed ‘/tftpboot/esr1x-1.6.0-build3.firmware’
```

Edit the file /etc/eltex-wifi-sa/factory-fw.conf by adding a definition for ESR-10 to it:

```
"ESR-10" {
min = 1.6.0.3
file = esr1x-1.6.0-build3.firmware
}
```

Restart the service:

```
root@softwlc-ott:/tftpboot# service eltex-wifi-sa restart
eltex-wifi-sa stop/waiting
eltex-wifi-sa start/running, process 29739
```

ISC-DHCP-SERVER

In OTT mode, ESR-10 uses suboption 15 of option 43 via which an address for GRE keepalived is sent. If an address with this option is received, an OTT connection is established successfully. In addition, a default route for management address will not be received that requires generation of a route to SoftWLC management core using option 121.
A default gateway's address for the management subnetwork (172.16.27.1 in the example given) will serve as an address, accessibility of which will be checked by GRE keepalive:

```
0F:0B:31:37:32:2e:31:36:2e:32:37:2e:31
```

In the OTT mode, ESR-10 will be connected to the same routers as access points do for GRE over IPsec termination. Therefore, during configuration of option 43, suboption 15 will be added to already existing option 10 via which an address of the SNMP server for access points is generated:

```
subnet 172.16.27.0 netmask 255.255.255.0 {
 pool {
  option routers 172.16.27.1;
  range 172.16.27.2 172.16.27.254;
  option vendor-encapsulated-options 0A:0E:31:39:32:2e:31:36:38:2e:34:32:2e:31:37:38:0f:0b:
31:37:32:2e:31:36:2e:32:37:2e:31;
  option ms-classless-static-routes 24, 192,168,42, 172,16,27,1;
  option rfc3442-classless-static-routes 24, 192,168,42, 172,16,27,1;
  option ntp-servers 192.168.42.178;
  allow members of "ELTEX-DEVICES";
}
}
```

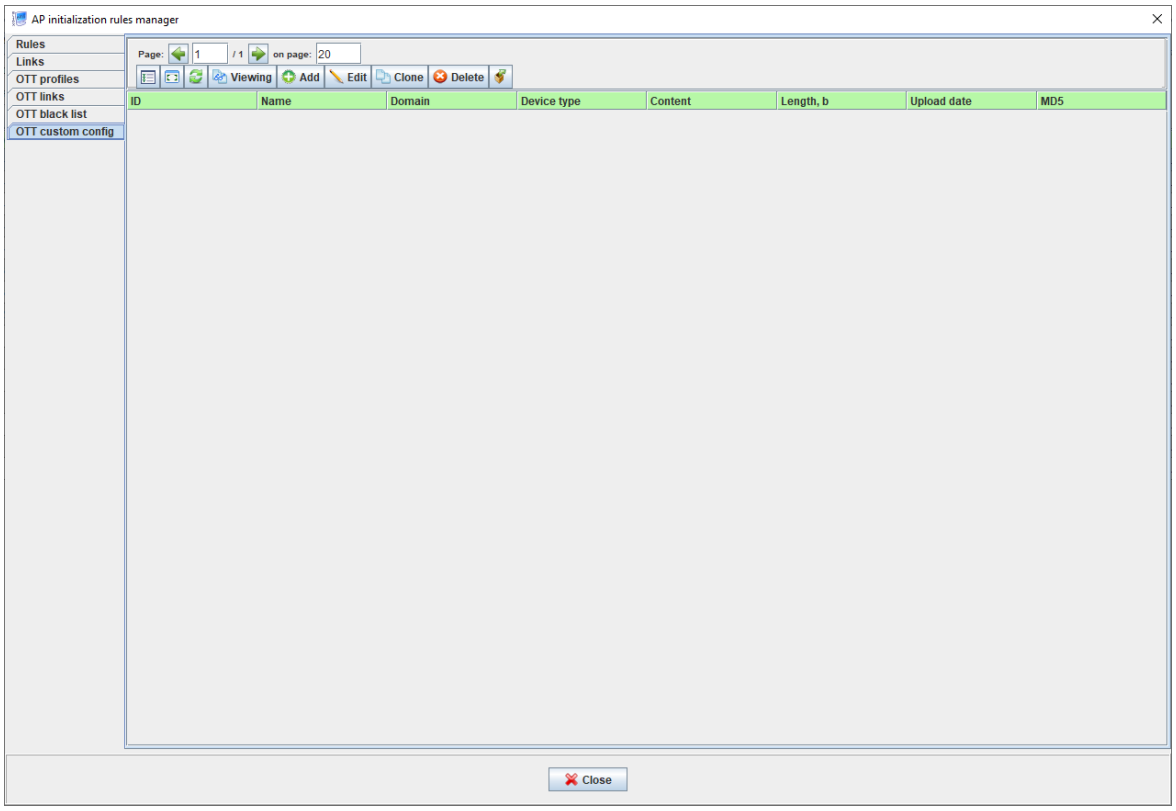
Do not forget to define ESR-10 in a rule allowing access only to devices of special types, if such a rule is used. In the example above, it is allow members of "ELTEX-DEVICES";

### Configuring connection and initialization using a default rule

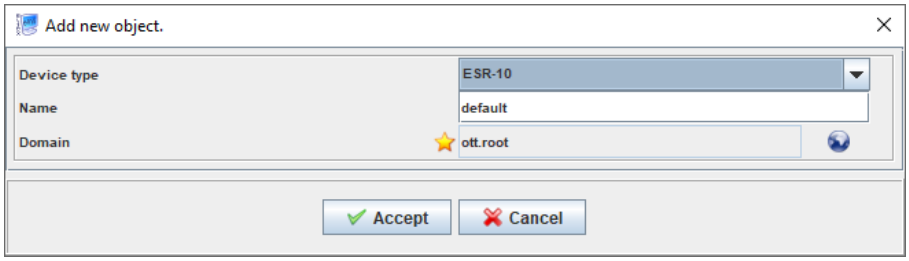
For the successful connection and initialization under a default rule, create a default configuration for ESR in the section "OTT custom config", create an initialization rule and specify ESR-10 in default link configuration.

#### EMS

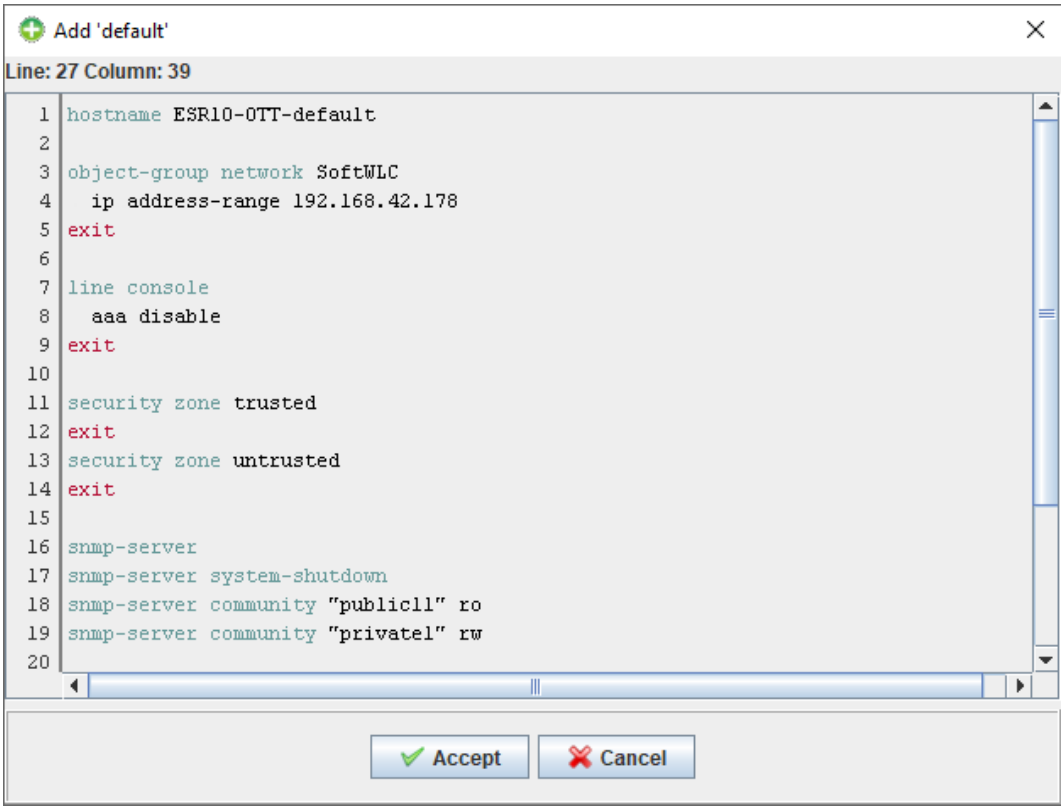
1. Open the menu "Wireless" → "AP initialization rules manager", select the tab "OTT custom config" and click "Add".




2. In the opened window, select "Domain", enter the name "default" (any name can be entered, this one just means that the rule will be used in default initialization link). "Device type" will already be selected (ESR-10). Click "Accept".



3. Add the default configuration and click "Accept".




ESR-10 default configuration:

**ESR-10 default configuration:**

*hostname ESR10-OTT-default*

*object-group network SoftWLC*
*ip address-range 192.168.42.178*
*exit*

*line console*
*aaa disable*
*exit*

*security zone trusted*
*exit*
*security zone untrusted*
*exit*

*snmp-server*
*snmp-server system-shutdown*
*snmp-server community "public11" ro*
*snmp-server community "private1" rw*

*snmp-server host 192.168.42.178*
*source-interface bridge 1*
*exit*

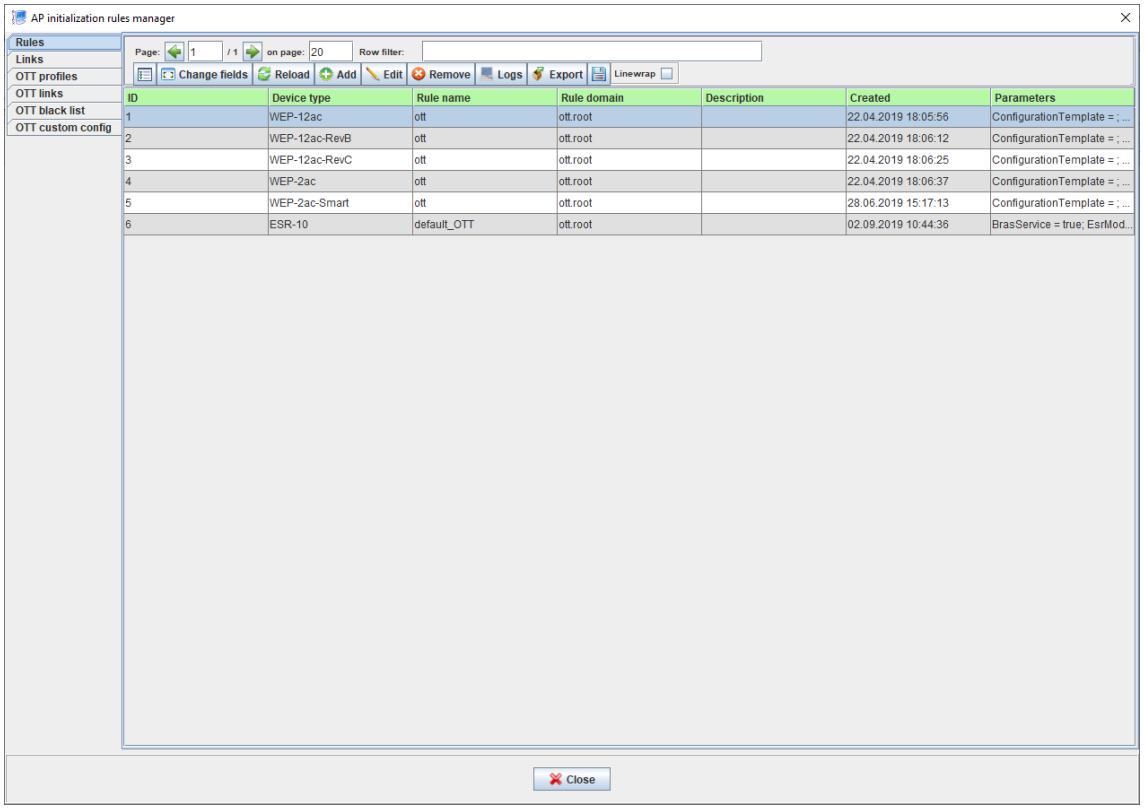
*snmp-server enable traps*
*snmp-server enable traps config*
*snmp-server enable traps config commit*
*snmp-server enable traps config confirm*
*snmp-server enable traps environment*
*snmp-server enable traps environment memory-flash-critical-low*
*snmp-server enable traps environment memory-flash-low*
*snmp-server enable traps environment memory-ram-critical-low*
*snmp-server enable traps environment memory-ram-low*
*snmp-server enable traps environment cpu-load*
*snmp-server enable traps environment cpu-critical-temp*
*snmp-server enable traps environment cpu-overheat-temp*
*snmp-server enable traps environment cpu-supercooling-temp*
*snmp-server enable traps file-operations*
*snmp-server enable traps file-operations successful*
*snmp-server enable traps file-operations failed*
*snmp-server enable traps file-operations canceled*
*snmp-server enable traps interfaces*
*snmp-server enable traps interfaces rx-utilization-high*
*snmp-server enable traps interfaces tx-utilization-high*
*snmp-server enable traps interfaces number-high*
*snmp-server enable traps screen*
*snmp-server enable traps screen dest-limit*
*snmp-server enable traps screen source-limit*
*snmp-server enable traps screen icmp-threshold*
*snmp-server enable traps screen udp-threshold*
*snmp-server enable traps screen syn-flood*
*snmp-server enable traps screen land*
*snmp-server enable traps screen winnuke*
*snmp-server enable traps screen icmp-frag*
*snmp-server enable traps screen udp-frag*
*snmp-server enable traps screen icmp-large*
*snmp-server enable traps screen syn-frag*
*snmp-server enable traps screen unknown-proto*
*snmp-server enable traps screen ip-frag*
*snmp-server enable traps screen port-scan*
*snmp-server enable traps screen ip-sweep*
*snmp-server enable traps screen syn-fin*
*snmp-server enable traps screen fin-no-ack*
*snmp-server enable traps screen no-flag*
*snmp-server enable traps screen spoofing*
*snmp-server enable traps screen reserved*
*snmp-server enable traps screen quench*
*snmp-server enable traps screen echo-request*
*snmp-server enable traps screen time-exceeded*

```
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore dns-nameserver
 ip dhcp client ignore router
 enable
exit

interface gigabitethernet 1/0/1
 description "UPLink"
 ip address dhcp
 security-zone untrusted
exit
interface gigabitethernet 1/0/2
 shutdown
exit
interface gigabitethernet 1/0/3
 shutdown
exit
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
```

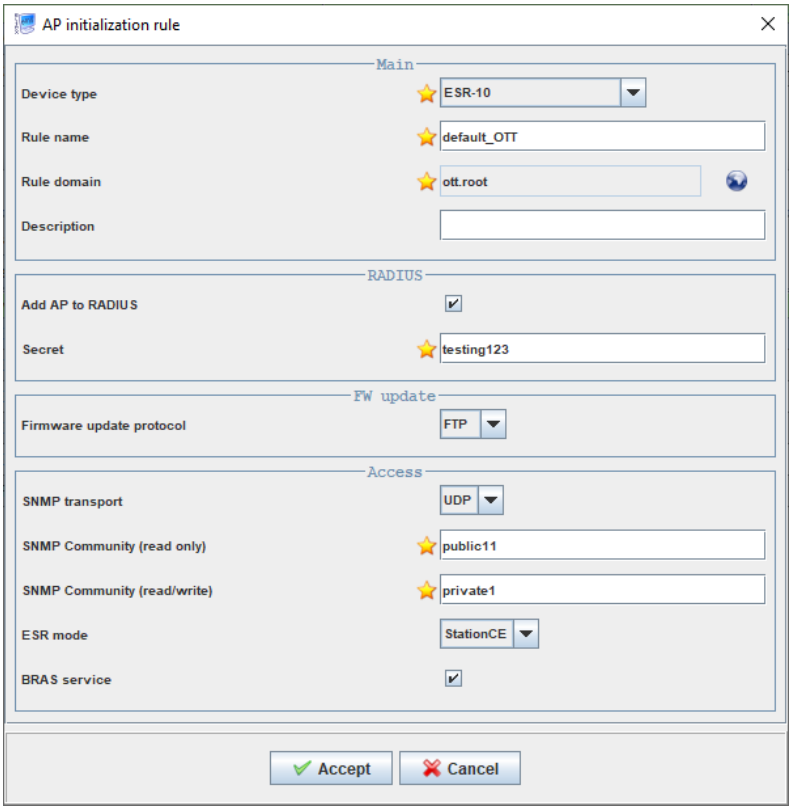
```
tunnel gre 1
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 mode ethernet
 local address xauth ipsec_vpn
 remote address xauth ipsec_vpn management-ip
 enable
exit
tunnel gre 1.1
 bridge-group 1
 snmp init-trap
 enable
exit

security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
  rule 1
   action permit
   match source-address SoftWLC
   enable
  exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
exit
```

```
security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
 proposal ipsec_prop
exit


security ipsec vpn ipsec_vpn
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

ip ssh server
```

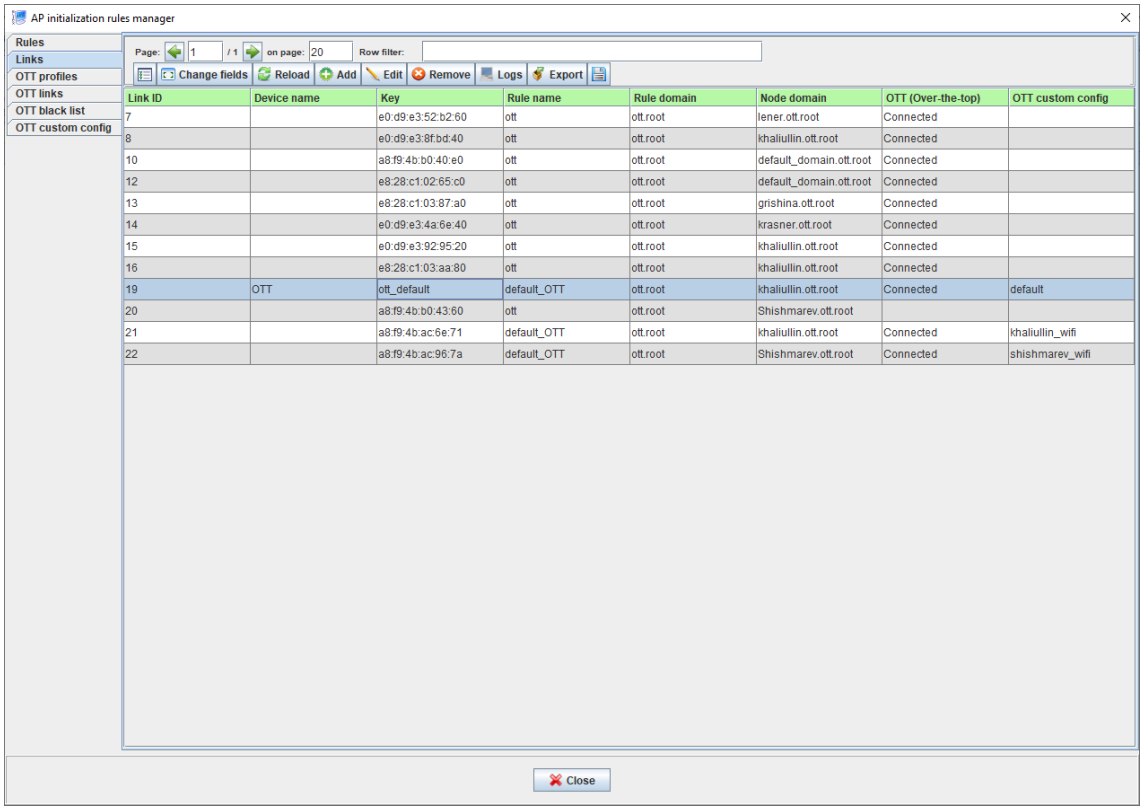
4. Open the menu "AP initialization rules manager", select the tab "Rules" and click "Add":




5. In the opened window:



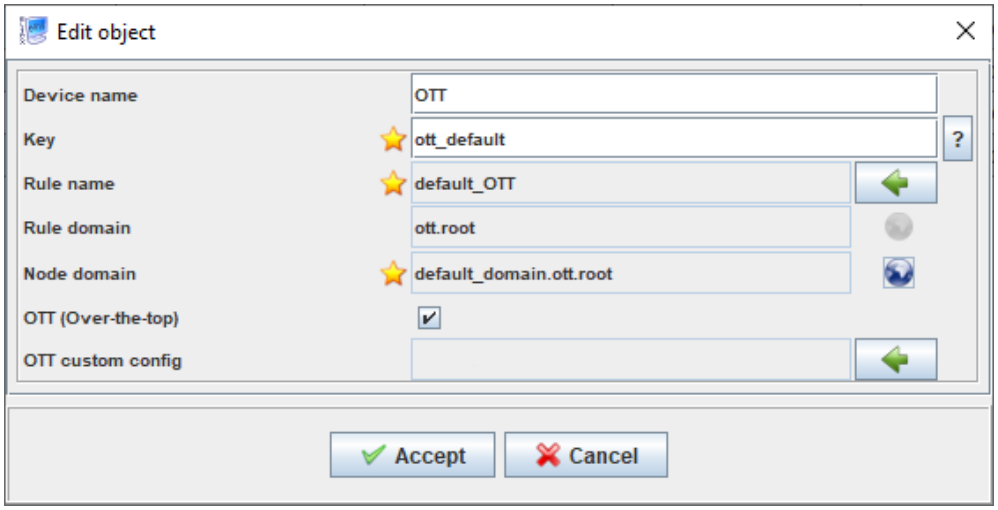

Select:
1) "Device type" - "ESR-10";
2) "Rule name" - "default OTT" (it is assumed that default OTT link was configured before to connect AP OTT using the same name);
3) "Add AP to RADIUS" - enable this checkbox;
4) "Secret" - "testing123";
5) "Firmware update protocol" - select "FTP";
6) "SNMP transport" - "UDP";
7) "SNMP Community (read only)" - "public11" (minimum community length on ESR is 8 characters);
8) "SNMP Community (read/write)" - "private1";
9) ESR mode - "StationCE" (a new parameter has been added, which means the device interacts with PCRF, and tunnel establishment is not required);
10) "BRAS service" - set this checkbox (ESR-10 in the OTT mode assumes working only with passing local client traffic to the network of the provider for which OTT device is connected).
And click "Accept".
6. In the menu "AP initialization rules manager", open the tab "Links" and select the default OTT link (it is assumed that it was configured before during congiguration of AP OTT connections):




| Link ID | Device name | Key | Rule name | Rule domain | Node domain | OTT (Over-the-top) | OTT custom config |
|---|---|---|---|---|---|---|---|
| 7 | | e0:d9:e3:52:b2:60 | ott | ott.root | lener.ott.root | Connected | |
| 8 | | e0:d9:e3:8f:bd:40 | ott | ott.root | khaliullin.ott.root | Connected | |
| 10 | | a8:f9:4b:b0:40:e0 | ott | ott.root | default_domain.ott.root | Connected | |
| 12 | | e8:28:c1:02:65:c0 | ott | ott.root | default_domain.ott.root | Connected | |
| 13 | | e8:28:c1:03:87:a0 | ott | ott.root | grishina.ott.root | Connected | |
| 14 | | e0:d9:e3:4a:6e:40 | ott | ott.root | krasner.ott.root | Connected | |
| 15 | | e0:d9:e3:92:95:20 | ott | ott.root | khaliullin.ott.root | Connected | |
| 16 | | e8:28:c1:03:aa:80 | ott | ott.root | khaliullin.ott.root | Connected | |
| 19 | OTT | ott_default | default_OTT | ott.root | khaliullin.ott.root | Connected | default |
| 20 | | a8:f9:4b:b0:43:60 | ott | ott.root | Shishmarev.ott.root | | |
| 21 | | a8:f9:4b:ac:6e:71 | default_OTT | ott.root | khaliullin.ott.root | Connected | khaliullin_wifi |
| 22 | | a8:f9:4b:ac:96:7a | default_OTT | ott.root | Shishmarev.ott.root | Connected | shishmarev_wifi |

and click "Edit".

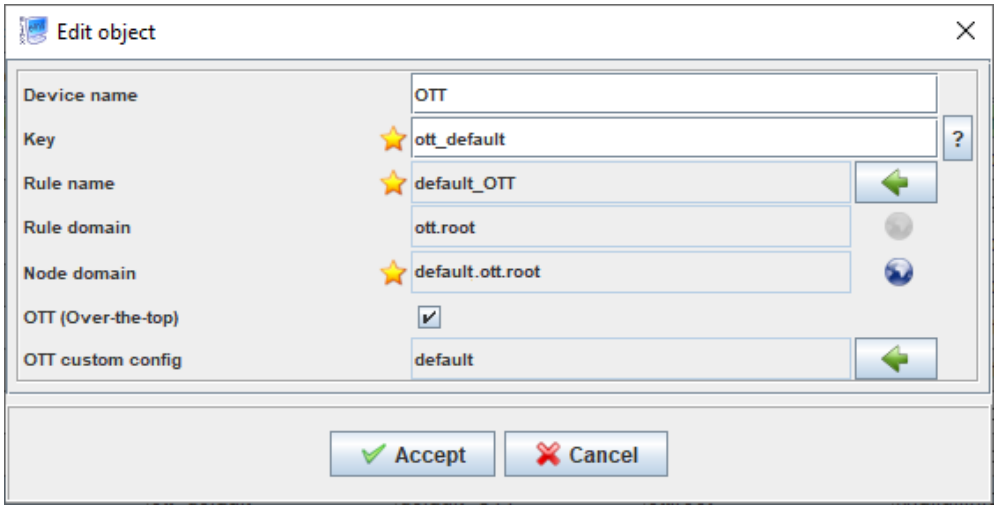
7. In the opened window, click the arrow on the right to select "OTT custom config" that will be used by ESR-10 after its connection to the SA.




8. Select the configuration "default" created before and click "Accept".

| ID | Name | Domain | Device type | Content | Length, b | Upload date | MD5 |
|---|---|---|---|---|---|---|---|
| 5d6c94808b12343c4c... | default | ott.root | ESR-10 | CLI | 4743 | Mon Sep 02 11:03:12 K... | b28a32f5a0b8ae9a76... |

9. Check the selected configuration:



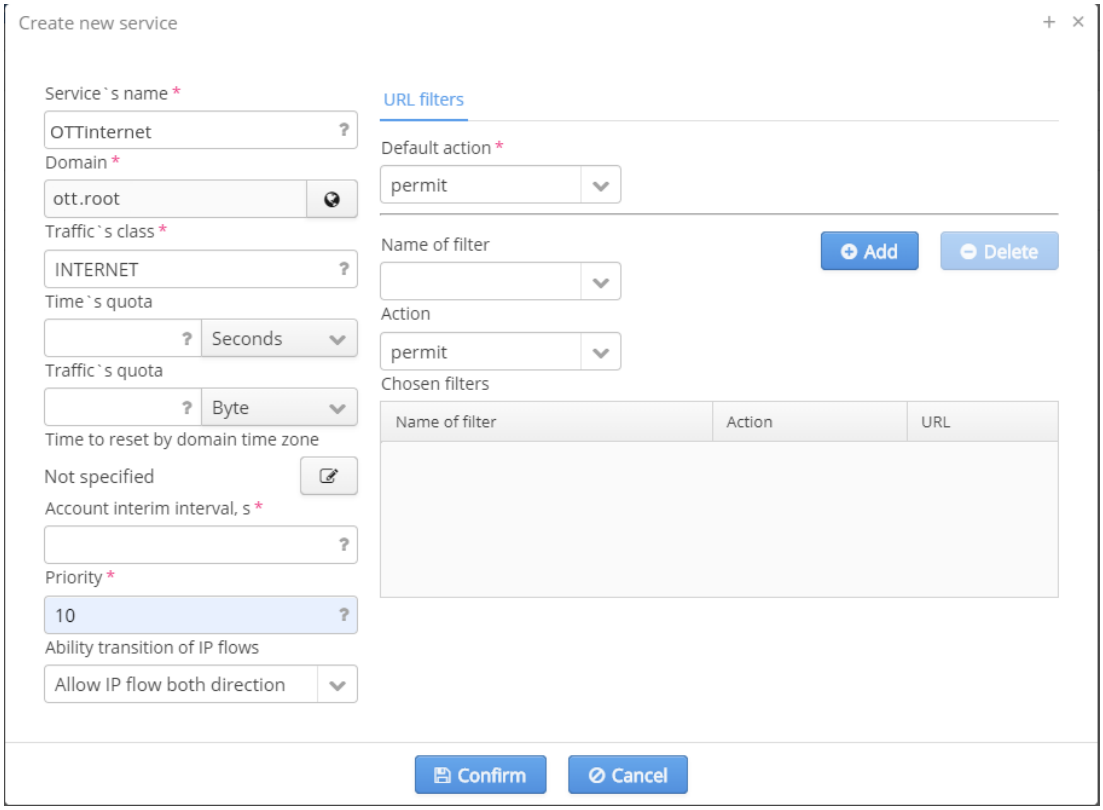

and click "Accept".
10. Close the window "AP initialization rules manager". Preconfiguration is completed. When connected, ESR-10 will be put into the default domain. After that, it can be put into a client domain and configured according to a client's requirements

## Connecting clients

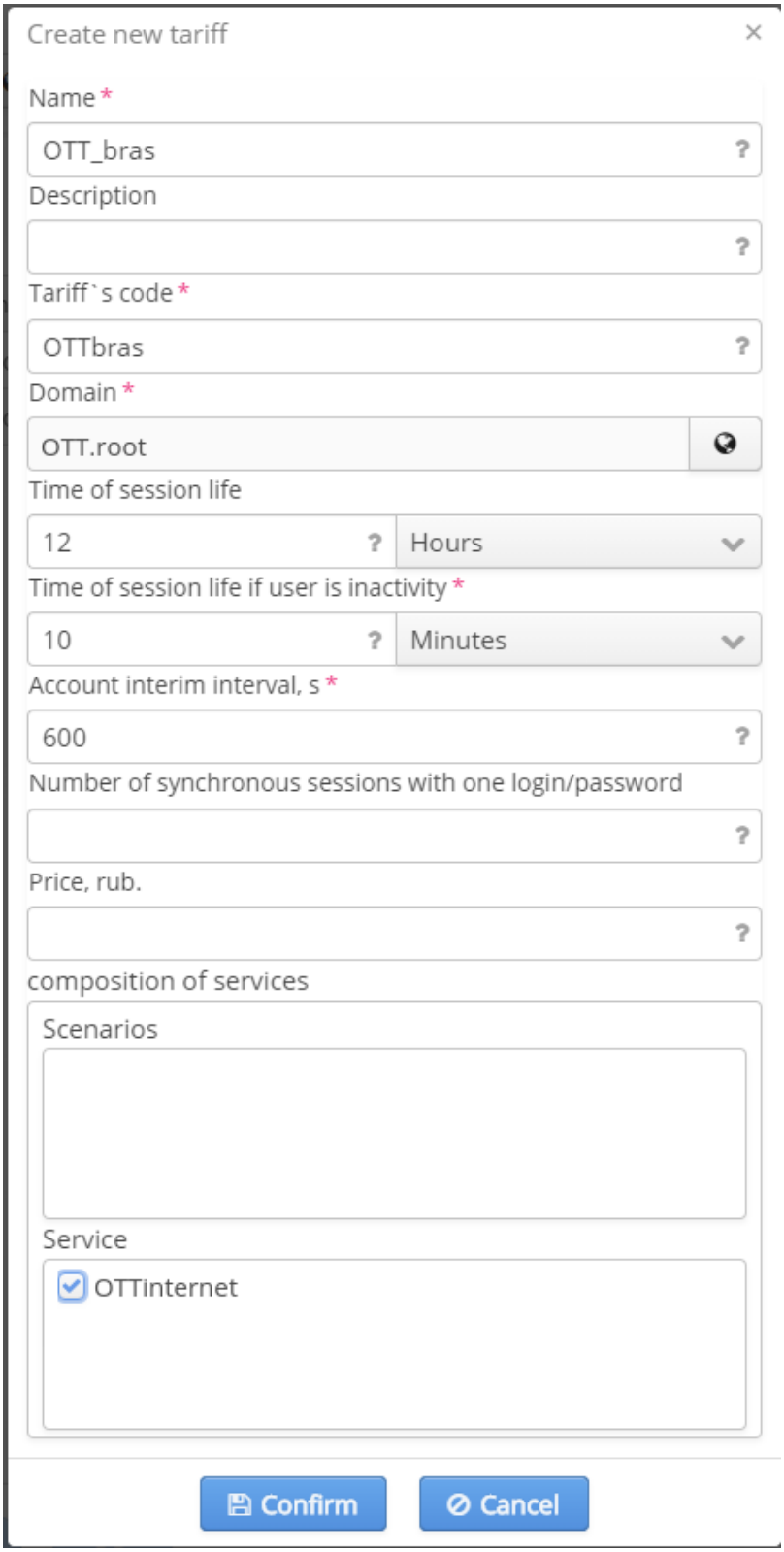
Before connecting a client, a connection scheme should be determined (how client traffic will pass from AP). Several ways are possible:
1) user traffic is tagged with a relevant vlan ID and sent to the uplink (gi1/0/1) of ESR-10 connection;
2) user traffic is untagged - in this case, only connection via the interfaces gi1/0/2 - gi1/0/6 is possible;
3) user traffic is tagged, but a special port (not uplink) gi1/0/2-gi1/0/6 ESR-10 is used for connection.
MAC address of ESR-10 that will be set up for a client can be either known or unknown. It will most likely be unknown, so in the example given below, ESR-10 will be put into a default domain by a default link at the first connection, then it will be moved into a required domain. Custom configuration will be assigned to an appeared link. Then reset will be performed for the ESR to get new information.
In the example given below, it is assumed that tagged traffic from a client's access points passes through ESR-10 uplink. Two SSID are used in their respective vlan: SSID 1 VID 701 and SSID2 VID 702, they come to the same bridge with location SSID12.

### Configuring BRAS services and tariffs

Configuration of services and tariffs is done in the same way as for the classic scheme with BRAS. Existing services and tariffs can be used. New ones can also be created. In the example given, it is assumed that a new service and tariff are created for the scheme with OTT. The WELCOME service remains the same.
1. Open the Admin Panel, select the tab "Services and tariffs" → "PCRF services" and click "Add":




1) "Service's name" - "OTTinternet";
2) "Domain" - specify a domain;
3) "Traffic's class" - "INTERNET";
4) "Account interim interval" - "600";
5) "Priority" - "10";
6) "Ability transition of IP flows" - select "Allow IP flow both direction".
Click "Save".
2. Open the tab "Services and tariffs" → "Tariffs", select a filter "PCRF/BRAS" and click "Add":




1) "Name" - tariff name;
2) "Tariff's code" - tariff code;

3) "Domain" - tariff domain (it should be the same as a domain of a service that will be used in the tariff);
4) "Time of session life" - "12" hours;
5) "Time of session life if user is inactive" - "10" minutes;
6) "Account interim interval" - "600" seconds;
7) "Services" - select the service "OTTinternet" configured before;
And click "Save".

### Portal configuration

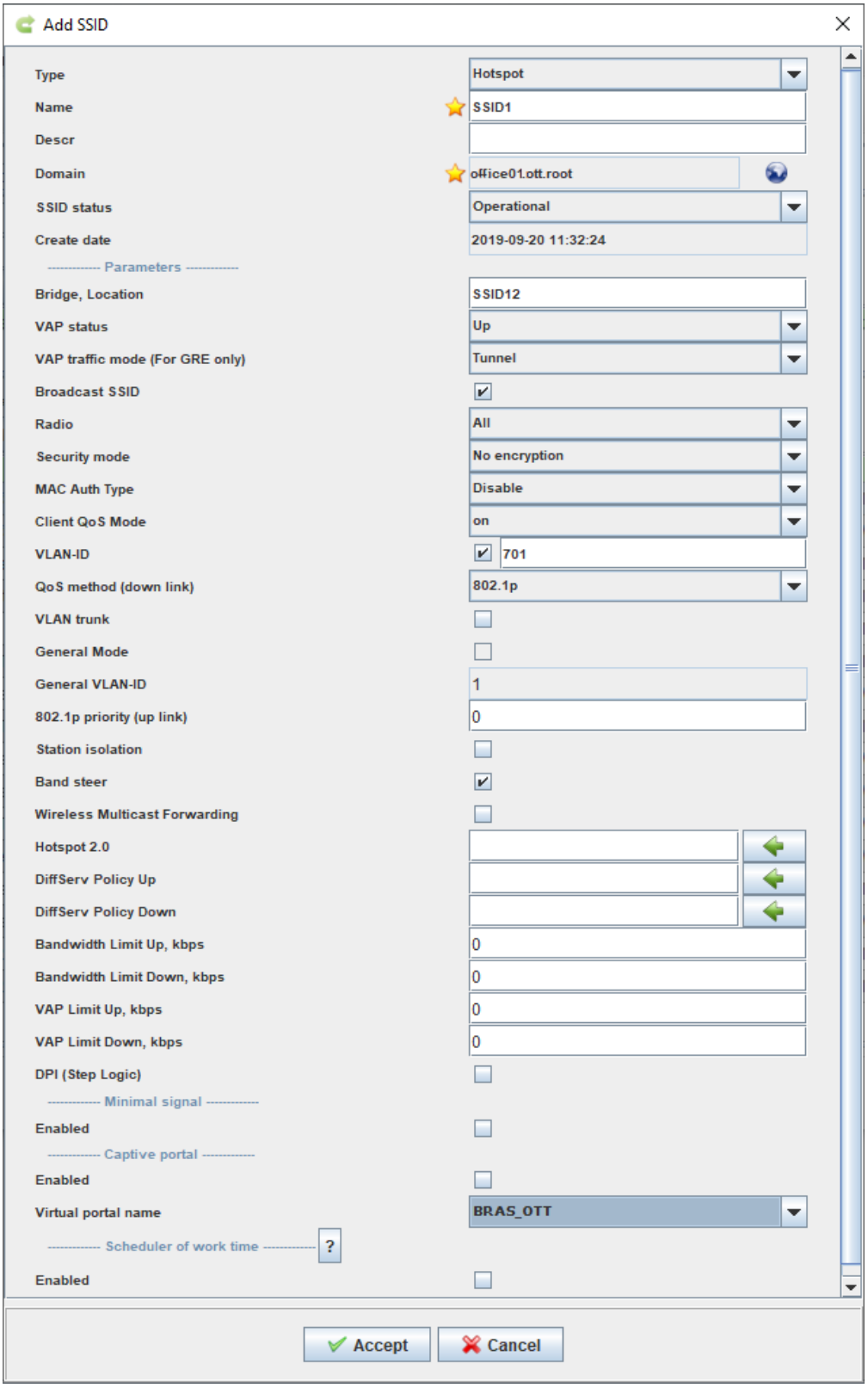
Portal configuration is done in the same way as for the classic scheme with BRAS. An existing portal can be used. New one can also be created. In the example below, a new portal will be created. BRAS interaction is assumed to have been configured.
1. Open the Portal Constructor, click "New portal":


1) "Virtual portal name" - enter the name;
2) "Domain" - select a domain;
Click "Save".
2. Open the menu "Tariffs". Delete the default tariff for AP and add the tariff "OTT_bras" created before.
Click "Save".

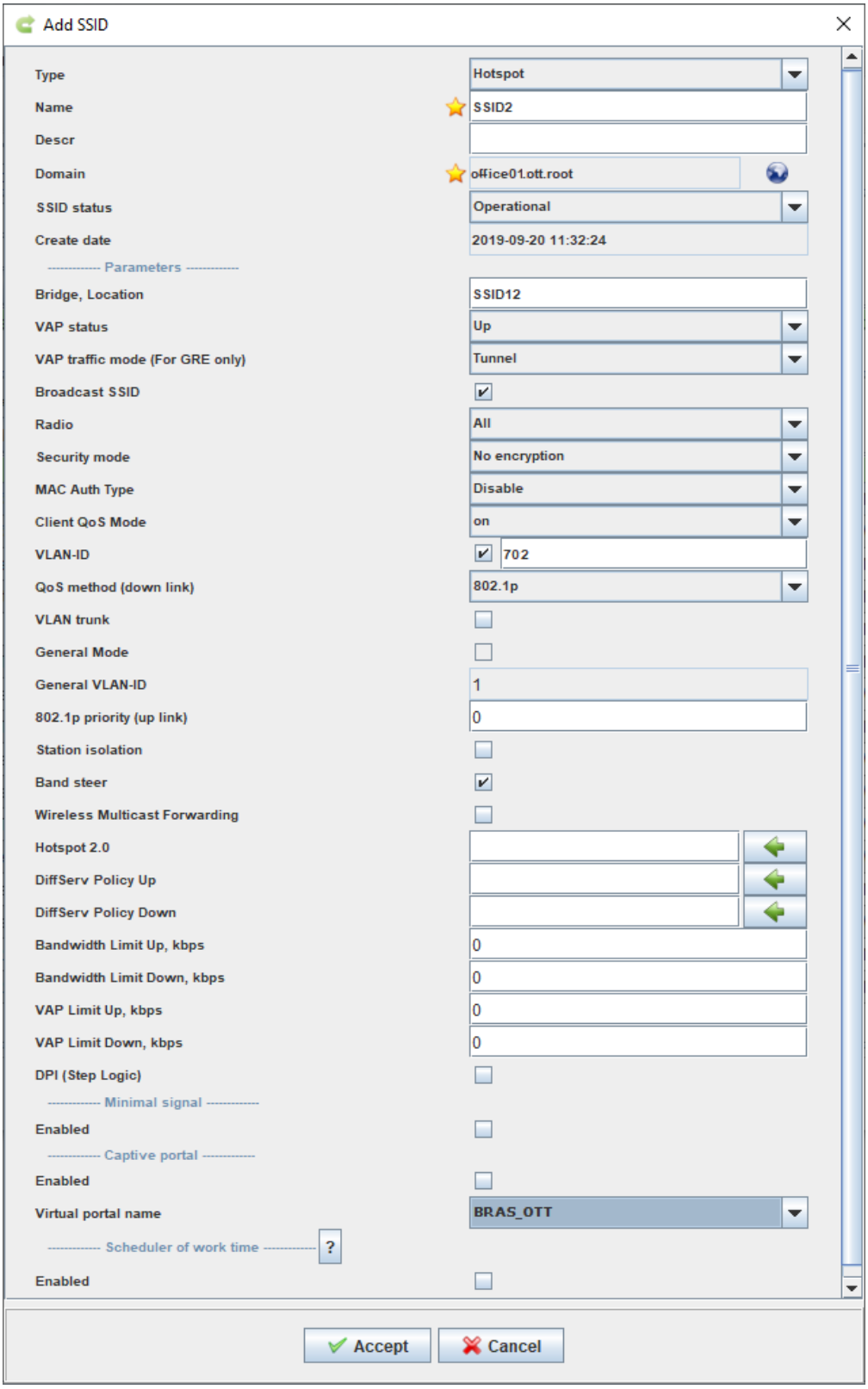
### Configuring SSID

SSID configuration and linking is done in the same way as for tariffs using BRAS: "Wireless" → "SSID Manager" → "Add SSID":

Configuring SSID1.
Select the mode "tunnel" in the field "VAP traffic mode" to provide an opportunity to use shapers on ESR-10 in BRAS mode (for such SSID shaper profiles are created).



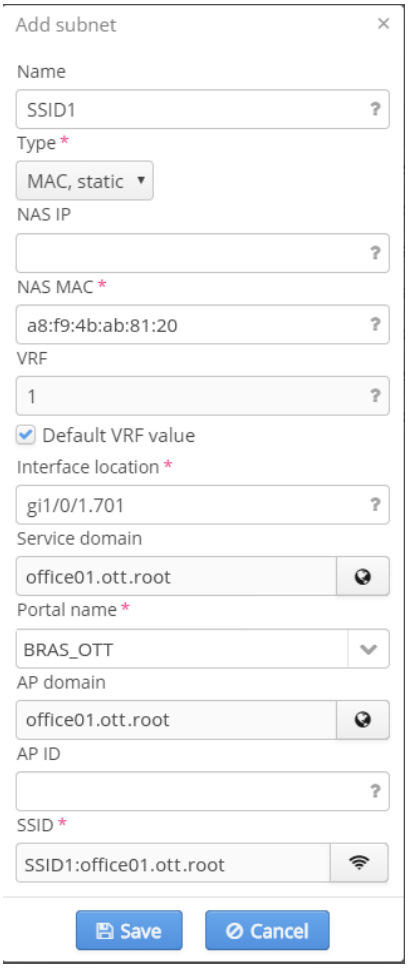

SSID2 is configured in a similar way:




Create links to a domain where ESR-10 will be put.

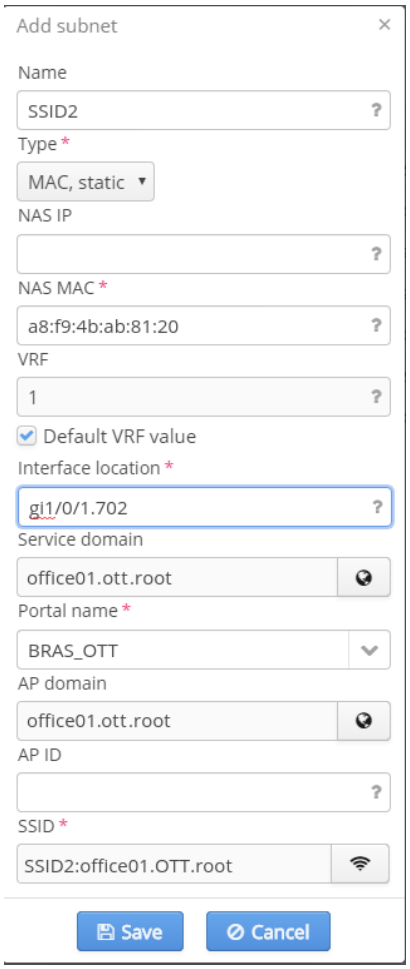
Creating L2 subnetworks

L2 subnetworks are created in the "Admin Panel". As IP address is assigned to a management device via DHCP, it can be changed during operation. To do this, a special type of L2 subnetworks has been implemented for the OTT scheme (and for any scheme using BRAS on ESR-10) - "MAC, static". The main marker for determining L2 subnetwork affiliation is NAS MAC. NAS IP is updated in the following cases:
1) management address is changed (SNMP trap of ESR-10 presence is sent to the same MAC from another address);
2) during initialization;
3) during reinitialization.
In these cases, the entry "Notify PCRF about IP changes for MAC-based subnets" will be added to the log.
In the example given, two L2 subnetworks will be required - for SSID1 and SSID2.
In the Admin Panel, open the tab "PCRF settings" → "L2 subnets" and click "Add":



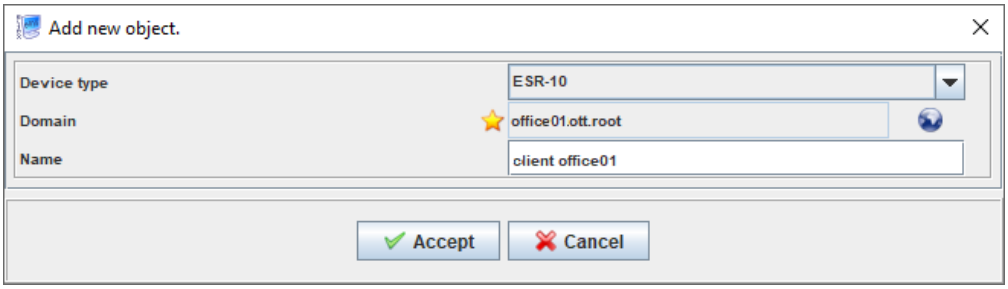

Enter:
Name - "SSID1";
1) "NAS IP" - do not fill (but if necessary, IP address can be specified or changed manually);
2) "Type" - select "MAC, static", enter ESR-10 MAC address;
3) "VRF" - check "Default VRF value";
4) "Location" - specify location gi1/0/1.701 (sub-interface to which traffic will come from SSID1);

5) "Service domain" - select SSID service domain;
6) "AP domain" - select a domain into which ESR-10 will be put.
7) "SSID" - select a required SSID (SSID1 in this case);
Click "Save".
Configure a L2 subnetwork for SSID2 in a similar way:



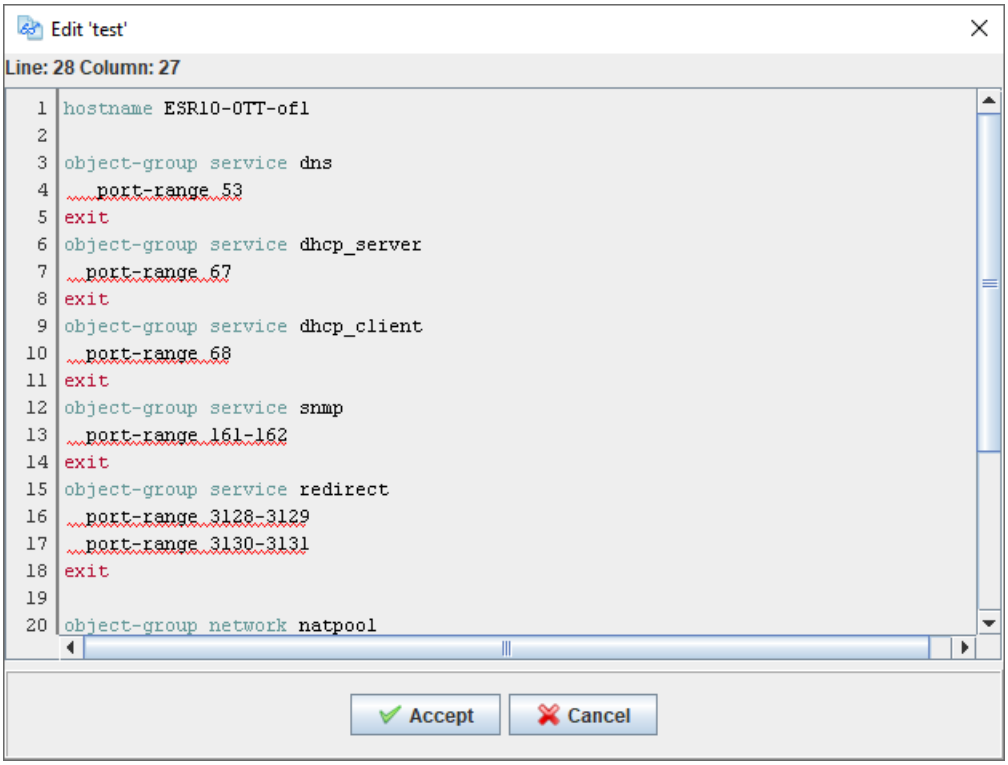

Creating OTT custom configuration

1. Open the menu "AP initialization rule manager", select the tab "OTT custom config" and click "Add":




Fill in the fields "Name" and "Domain", the field "Device type" will be already filled with "ESR-10". Click

"Accept".
2. In the opened window, specify the configuration:




**Configuration**

```
hostname ESR10-OTT-of1

object-group service dns
  port-range 53
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service snmp
 port-range 161-162
exit
object-group service redirect
 port-range 3128-3129
 port-range 3130-3131
exit

object-group network natpool
 ip prefix 192.168.1.0/24
exit
object-group network SoftWLC
```

```
 ip address-range 192.168.42.178
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
 key ascii-text encrypted 88B11079B9014FAAF7B9
 timeout 11
 priority 20
 source-interface bridge 1
 auth-port 31812
 acct-port 31813
 retransmit 10
  dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 192.168.42.178
exit
das-server COA
 key ascii-text encrypted 88B11079B9014FAAF7B9
 port 3799
 clients object-group SoftWLC
exit
aaa das-profile COA
 das-server COA
exit
line console
 aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
 rule 1
  action permit
  match protocol tcp
  match destination-port 443
  enable
 exit
 rule 2
  action permit
  match protocol tcp
  match destination-port 8443
```

```
  enable
 exit
 rule 3
  action permit
  match protocol tcp
  match destination-port 80
  enable
 exit
 rule 4
  action permit
  match protocol tcp
  match destination-port 8080
  enable
 exit
exit

ip access-list extended INTERNET
  rule 1
  action permit
  enable
 exit
exit

ip access-list extended unauthUSER
 rule 1
  action permit
  match protocol udp
  match source-port 68
  match destination-port 67
  enable
 exit
 rule 2
  action permit
  match protocol udp
  match destination-port 53
  enable
 exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
 aaa das-profile COA
 aaa sessions-radius-profile PCRF
 aaa services-radius-profile PCRF
 nas-interface bridge 1
 session mac-authentication
 bypass-traffic-acl unauthUSER
 default-service
  class-map unauthUSER
  filter-name remote gosuslugi
```

```
  filter-action permit
  default-action redirect http://192.168.42.178:8080/eltex_portal/
  session-timeout 600
 exit
 enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
 source-interface bridge 1
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
```

```
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore dns-nameserver
 ip dhcp client ignore router
 enable
exit
bridge 11
 security-zone user
 ip address 192.168.1.1/24
 service-subscriber-control any
 location SSID12
 enable
exit

interface gigabitethernet 1/0/1
 description "UPLink"
```

```
 ip address dhcp
 security-zone untrusted
exit
interface gigabitethernet 1/0/1.701
  bridge-group 11
exit
interface gigabitethernet 1/0/1.702
 bridge-group 11
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface gigabitethernet 1/0/3
 shutdown
exit
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
tunnel gre 1
 keepalive retries 3
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 mode ethernet
 local address xauth ipsec_vpn
 remote address xauth ipsec_vpn management-ip
enable
exit
tunnel gre 1.1
  bridge-group 1
 snmp init-trap
 enable
exit

security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
```

```
 rule 1
  action permit
  enable
 exit
exit
security zone-pair user untrusted
 rule 10
  action permit
  enable
 exit
exit
security zone-pair user self
 rule 10
  action permit
  match protocol udp
  match source-port dhcp_client
  match destination-port dhcp_server
  enable
 exit
 rule 20
  action permit
  match protocol tcp
  match destination-port redirect
  enable
 exit
 rule 30
  action permit
  match protocol udp
  match destination-port dns
  enable
 exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote network dynamic client
```

```
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
 proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

nat source
 ruleset NAT
  to interface gigabitethernet 1/0/1
  rule 10
   match source-address natpool
   action source-nat interface
   enable
  exit
 exit
exit

ip dhcp-server
ip dhcp-server pool lan
 network 192.168.1.0/24
 max-lease-time 000:00:20
 default-lease-time 000:00:10
 address-range 192.168.1.2-192.168.1.254
 default-router 192.168.1.1
 dns-server 192.168.1.1
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.123.0.2
exit
```

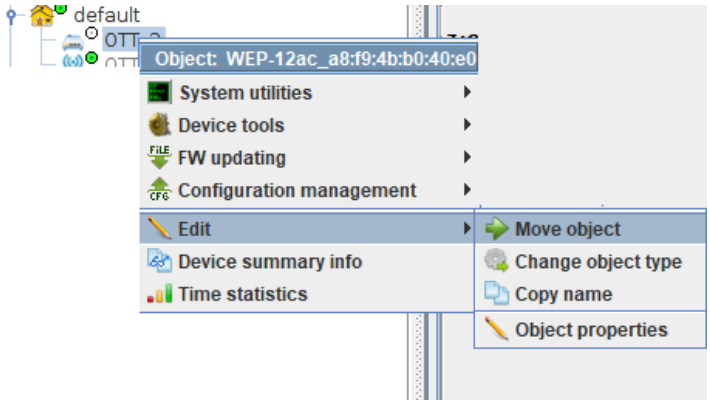
and click "Accept".

Creating a link for ESR-10 with OTT custom configuration

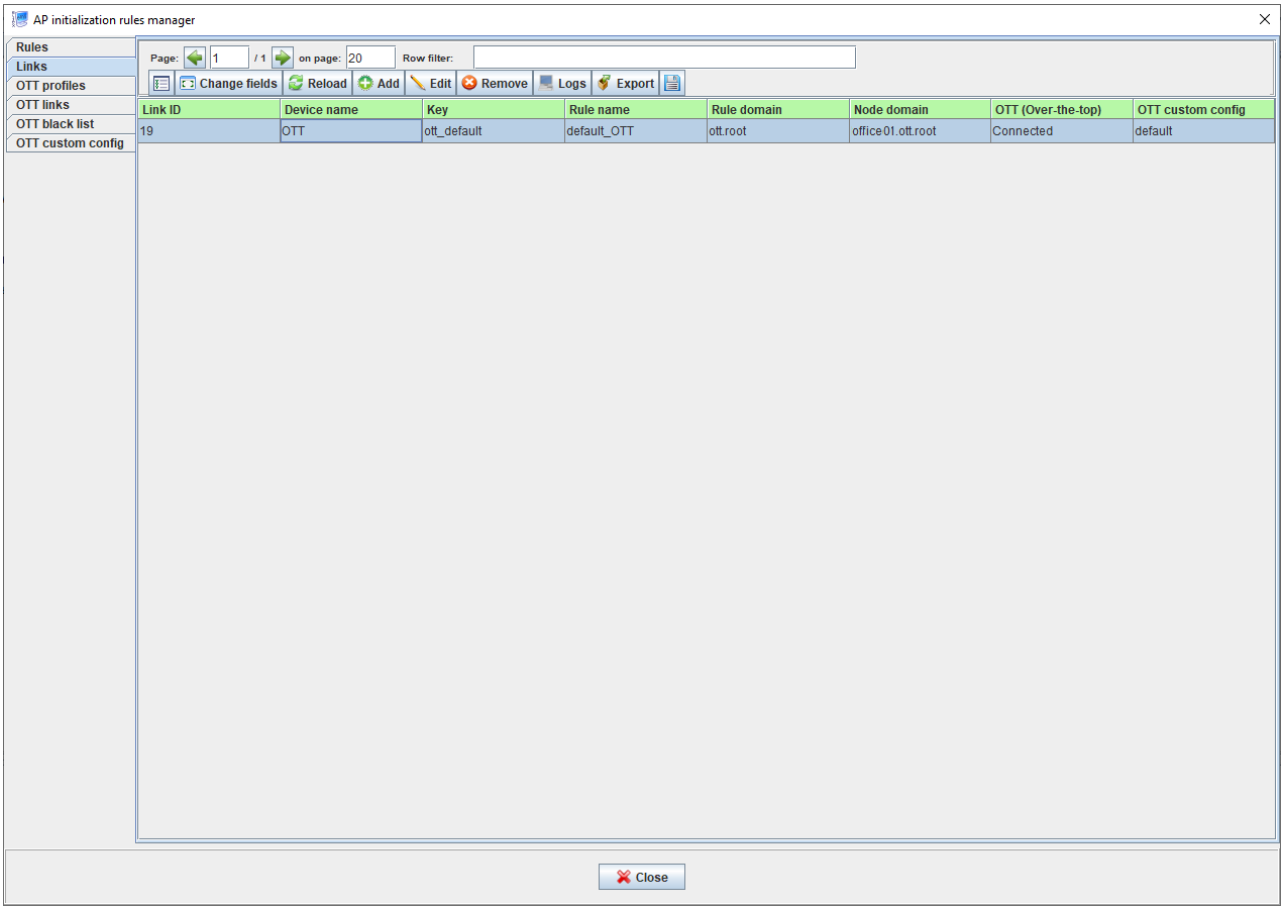
A link between OTT custom configuration and ESR can be created in two ways:

1) A default OTT link was used for ESR-10, and it was put into the default domain

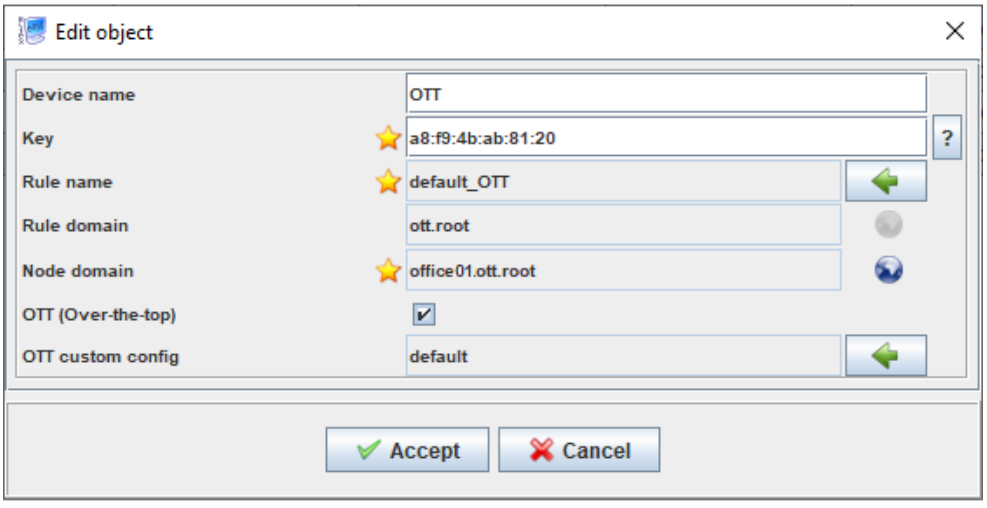
In thic case, ESR-10 MAC address becomes known after device installation.
1. Find it in the OTT device initialization default domain, select it and put into a required domain:



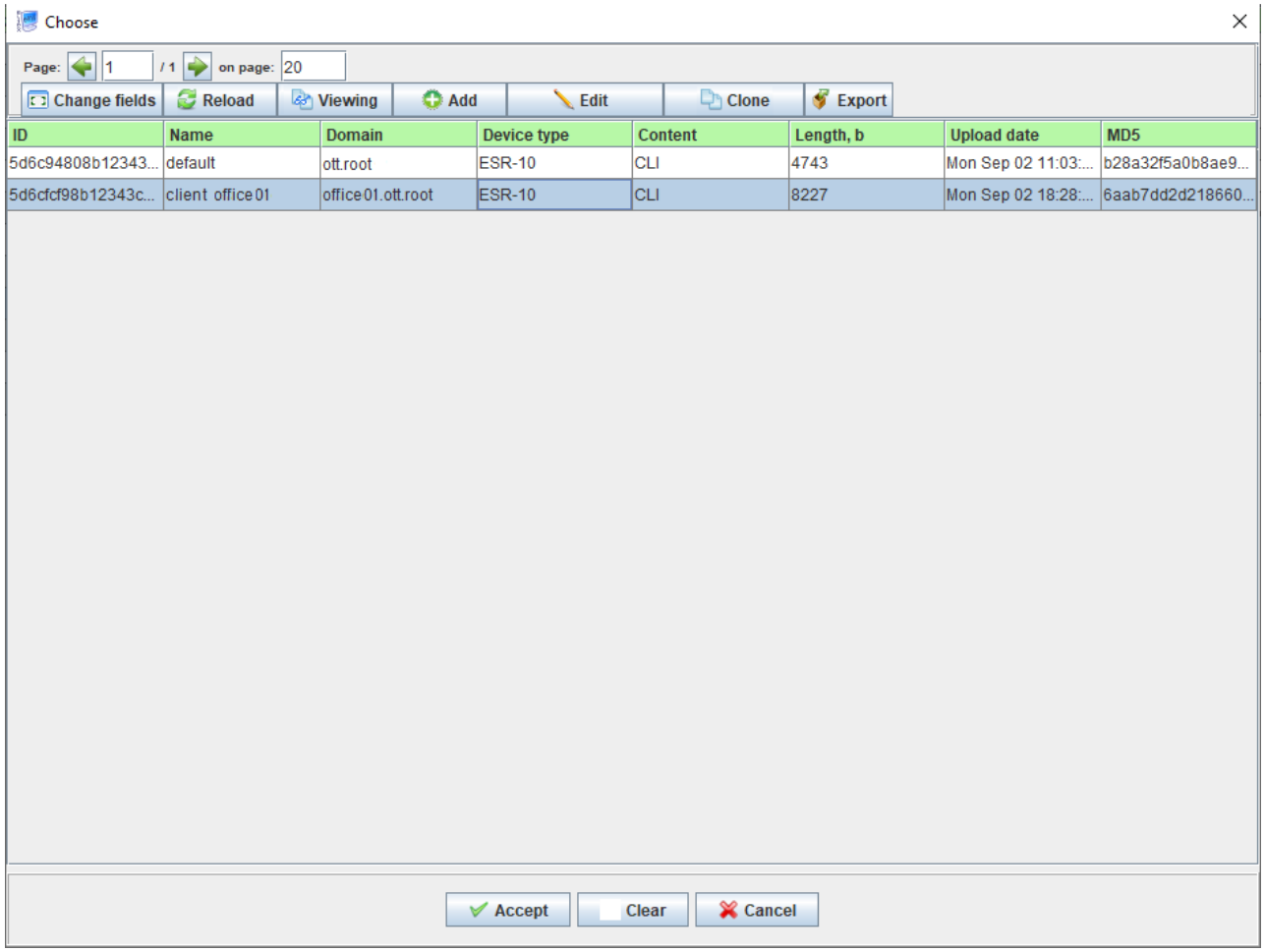

after the device is moved, A custom OTT link will be created.
2. Open "Wireless" → "AP initialization rules manager" → "OTT links" and find a link:




3. Select the link found and click "Edit":

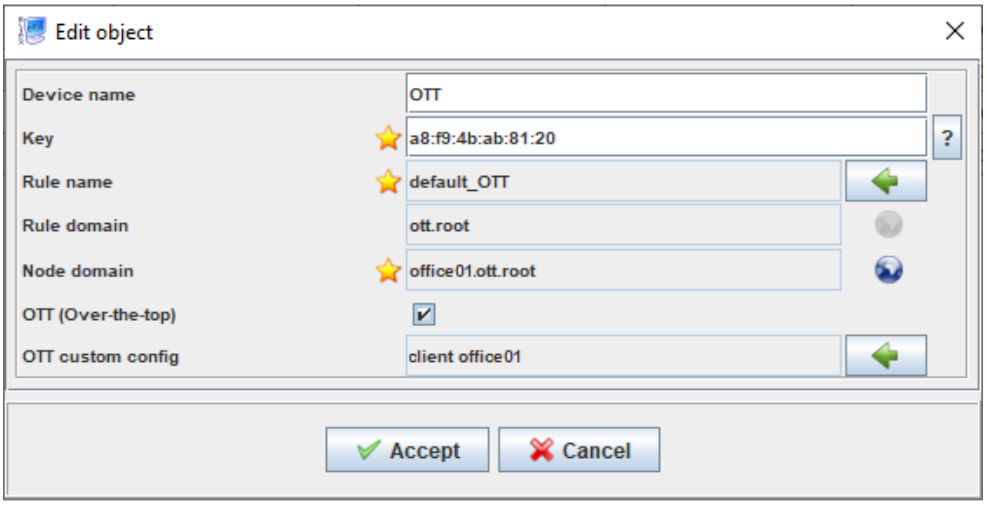



4. In the opened window, click the arrow to the right of "OTT custom config" and select a configuration corresponding to this ESR-10 in the opened window.



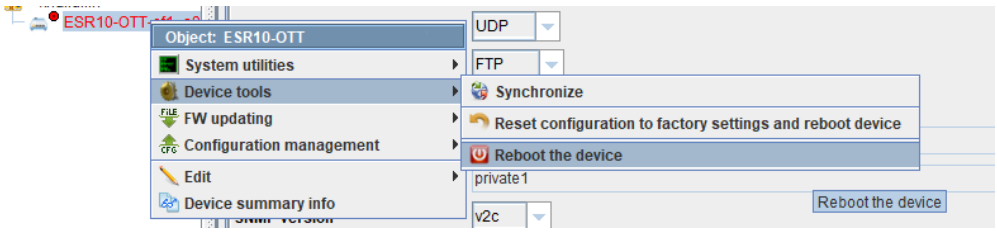

click "Accept".

5. "OTT custom config" has changed for this link:

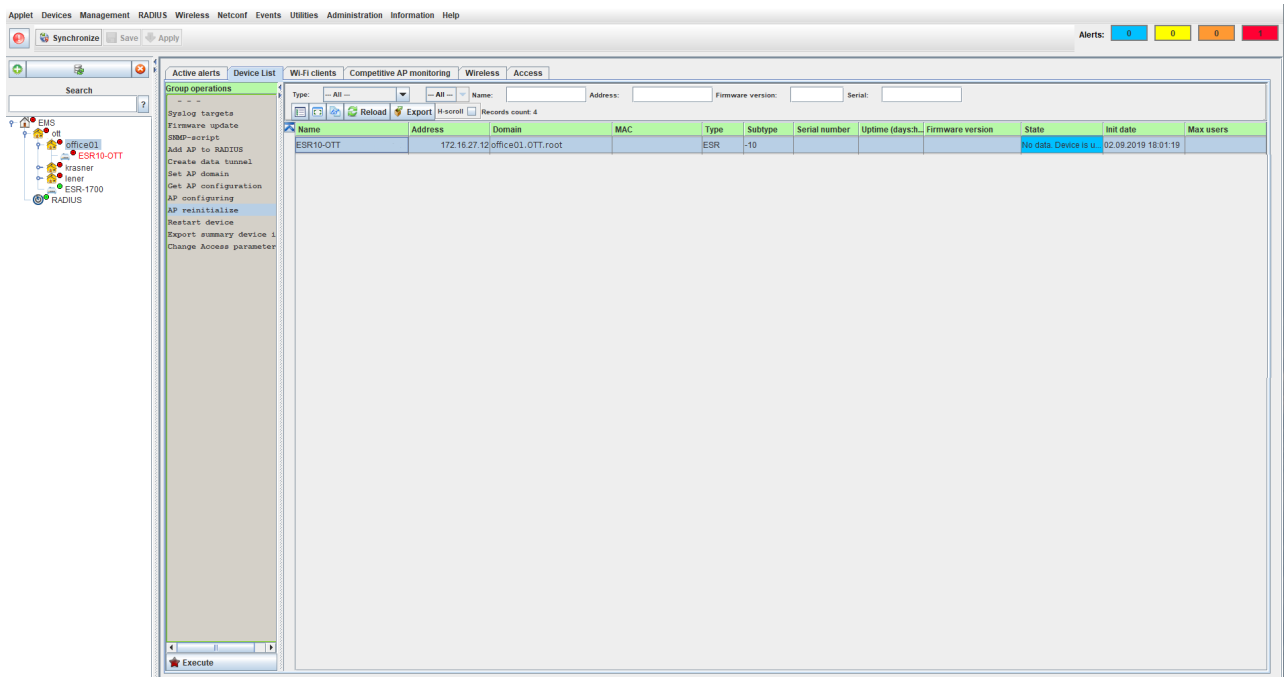



click "Accept".

Close "AP initialization rule manager".
5. Click the right mouse button on "ESR-10" and select "Device tools" → "Reboot the device".



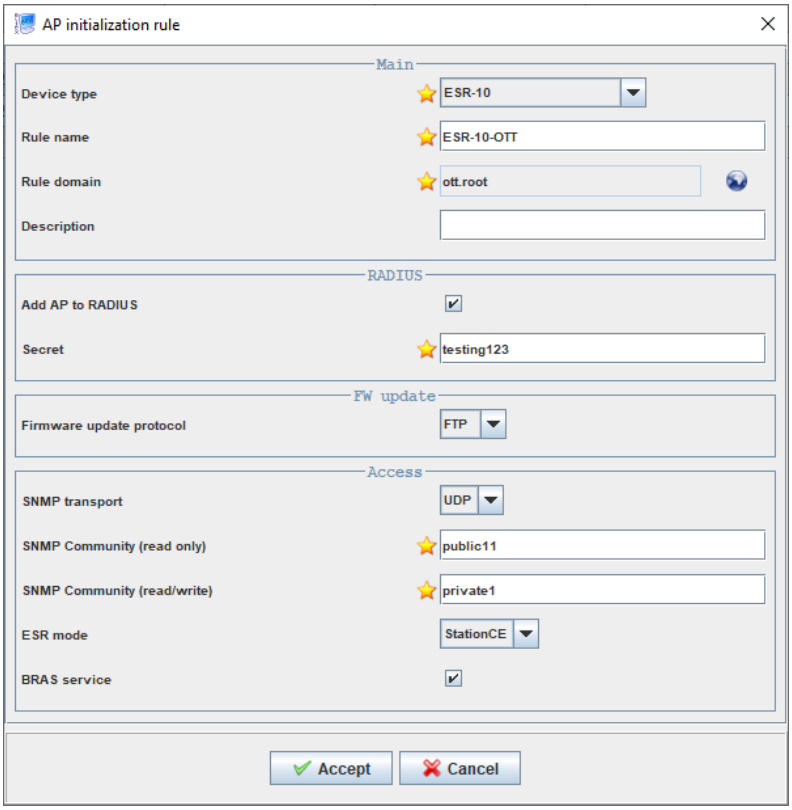

After some time, the device will reset, request the SA and get a new configuration.
6. After device configuration, perform reinitialization by rule link. To do this, select a domain where the device is initialized, open the tab "Device list" and select ESR-10 in the section "Group operations" → "AP reinitialization by rule". Click "Execute":



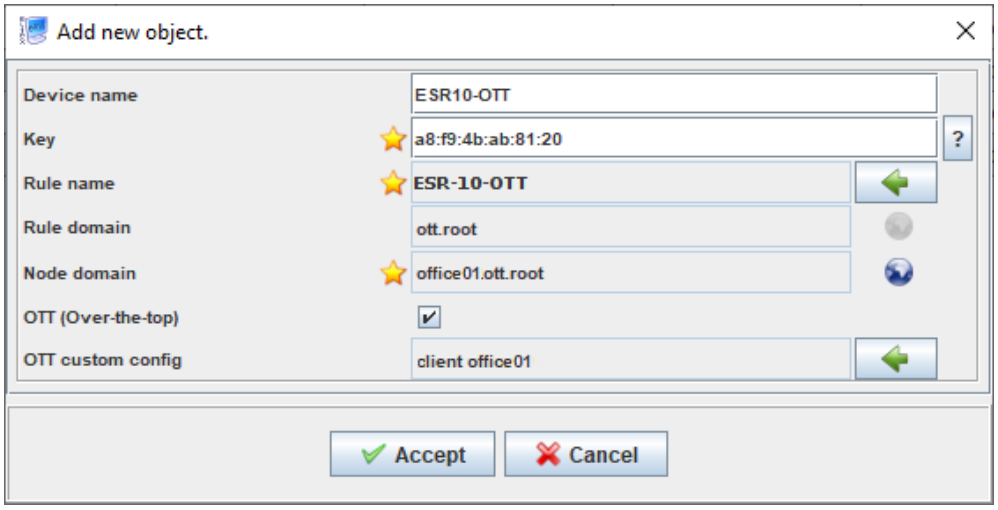

The status of implementation can be seen in the panel "Tasks" of the appeared task.
7. After that, the device is ready to go - performance check can be done.

2) Default OTT link is not used in EMS configuration, or MAC address of a device installed at a client's is known in advance.

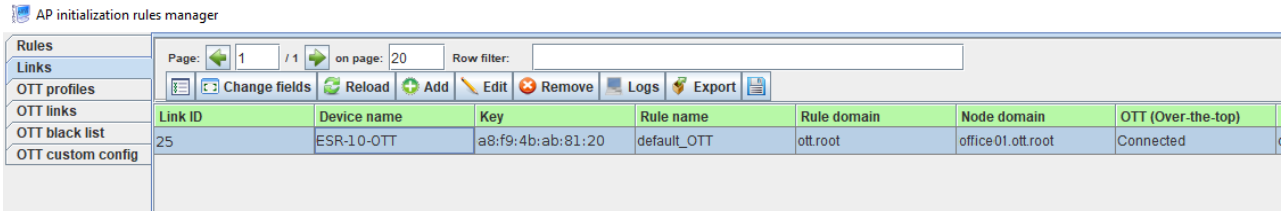
1. Creating an initialization rule for ESR-10 in the OTT mode. Open the tab "Wireless" → "AP initialization rules manager" → "Rules" and click "Add":




Select:
1) "Device type" - "ESR-10";
2) "Rule name" - "ESR-10-OTT" (another name can be specified);
3) "Add AP to RADIUS" - enable this checkbox;
4) "Secret" - "testing123";
5) "Firmware update protocol" - select "FTP";
6) "SNMP transport" - "UDP";
7) "SNMP Community (read only)" - "public11" (minimum community length on ESR is 8 characters);
8) "SNMP Community (read/write)" - "private1";
9) ESR mode - "StationCE" (a new parameter has been added, which means the device interacts with PCRF, and tunnel establishment is not required);
10) "BRAS service" - set this checkbox (ESR-10 in the OTT mode assumes working only with passing local client traffic to the network of the provider for which OTT device is connected).
And click "Accept".
2. Open the tab "Wireless" → "AP initialization rules manager" → "Links" and click "Add":




In the opened window specify:
1) "Device name" - the name that will be displayed in EMS;
2) "Key" - ESR-10 MAC address;
3) "Rule name" - select an initialization rule created before;
4) "Node domain" - specify the domain for device initialization;
5) OTT (Over-the-top) - enable this checkbox;
6) OTT custom config - select configuration created for the client.
Click "Accept":




It can be seen that initialization rule link has been performed successfully.
ESR-10 will be initialized within a required domain and ready to go right after its activation.

## Appendices

### Configuring OTT custom config, sent by the Service Activator

#### General description

Configuration received by ESR-10 from the Service Activator (hereinafter the "SA") consists of two parts - the first one contains IPsec parameters, update-timer, wait-timer, administrator password (admin) in JSON format. The second part contains CLI configuration in text format as set of CLI commands. All the parameters are keeped in one file.
If a part containing CLI in SA response received is empty, an error has occurred. This configuration will not be applied, an error code will be sent to the SA. ESR-10 will request the SA upon wait-timer expiry.
If a configuration contains wrong and non-existent commands, such a configuration will not be applied, an error code will be sent to the SA. ESR-10 will request the SA upon wait-timer expiry.

If a configuration contains incomplete settings that require other settings to be enabled, such a configuration will be applied, but incomplete settings will not be enabled.
If a configuration contains settings that are also passed by the Service Activator in IPsec connection parameters, the ones specified in the configuration will be used.
Configuration received by ESR-10 from the SA in the CLI part, is created in the tab "OTT custom config" of the meny "AP initialization rules manager". Parts of configuration containing uplink, IPsec, GRE settings, should be described in a certain way. Their change is unacceptable, as it will lead to configuration disability after applying (in this case, ESR will rollback to factory-config via ESR-10 wait-timer and send the error message to the SA).
OTT connection establishment implies having suboption 15 of option 43 when getting an address by the management interface (it will always be bridge 1). If an address with this option has not been received during wait-timer, connection is considered as failed. Configuration will rollback to factory-config, and the error message will be sent to the Service Activator. A request to the Service Activator will be repeated on the wait-timer expiry.
Untagged client traffic from SSID should not be passed via uplinks.
It is recommended to use a bridge with subinterfaces or physical interfaces for client termination. If BRAS is used on a physical interface or on a subinterface, it will require configuring two L2 subnetworks for each interface (the first subnetwork will contain location with the interface; the second one will contain the interface in the format of gi1/0/2 or gi1/0/2.100)

### Description of default configuration in the OTT custom config

For a default initialization rule, create a configuration "default" and provide a minimum necessary configuration to establish IPsec, get a management address and sent a presence trap to the system. Configuration name may differ. ESR-10 will appear in the default domain with this configuration. There will be an opportunity to manage it via EMS, but clients cannot work with this configuration. This configuration will be used only in situations when MAC address of a client's ESR-10 is unknown. After that, ESR-10 should be put into another domain. Another custom link will be created for it, and it will be possible to choose another custom configuration. A custom link can be also created in advance with required configuration provided for a client.
An example of ESR-10 configuration after applying parameters from SA is given below. Parameters that should not be specified in "OTT custom config" are shaded gray.

```
hostname ESR10-OTT

object-group network SoftWLC
 ip address-range 192.168.42.178
exit

line console #Deny access fron the console to ESR10
 aaa disable
exit

security zone trusted
exit
security zone untrusted
exit
```

*snmp-server*
*snmp-server system-shutdown*
*snmp-server community "public11" ro*
*snmp-server community "private1" rw*

*snmp-server host 192.168.42.178*
*source-interface bridge 1*
*exit*

*snmp-server enable traps*
*snmp-server enable traps config*
*snmp-server enable traps config commit*
*snmp-server enable traps config confirm*
*snmp-server enable traps environment*
*snmp-server enable traps environment memory-flash-critical-low*
*snmp-server enable traps environment memory-flash-low*
*snmp-server enable traps environment memory-ram-critical-low*
*snmp-server enable traps environment memory-ram-low*
*snmp-server enable traps environment cpu-load*
*snmp-server enable traps environment cpu-critical-temp*
*snmp-server enable traps environment cpu-overheat-temp*
*snmp-server enable traps environment cpu-supercooling-temp*
*snmp-server enable traps file-operations*
*snmp-server enable traps file-operations successful*
*snmp-server enable traps file-operations failed*
*snmp-server enable traps file-operations canceled*
*snmp-server enable traps interfaces*
*snmp-server enable traps interfaces rx-utilization-high*
*snmp-server enable traps interfaces tx-utilization-high*
*snmp-server enable traps interfaces number-high*
*snmp-server enable traps screen*
*snmp-server enable traps screen dest-limit*
*snmp-server enable traps screen source-limit*
*snmp-server enable traps screen icmp-threshold*
*snmp-server enable traps screen udp-threshold*
*snmp-server enable traps screen syn-flood*
*snmp-server enable traps screen land*
*snmp-server enable traps screen winnuke*
*snmp-server enable traps screen icmp-frag*
*snmp-server enable traps screen udp-frag*
*snmp-server enable traps screen icmp-large*
*snmp-server enable traps screen syn-frag*
*snmp-server enable traps screen unknown-proto*
*snmp-server enable traps screen ip-frag*
*snmp-server enable traps screen port-scan*
*snmp-server enable traps screen ip-sweep*
*snmp-server enable traps screen syn-fin*
*snmp-server enable traps screen fin-no-ack*

```
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1 #bridge 1 will also be used for management, settings should remain the same
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore router
 enable
exit

interface gigabitethernet 1/0/1 #The interface gi1/0/1 will always be used as an uplink, settings
should remain the same
 description "UPLink"
 ip address dhcp
 security-zone untrusted
exit
interface gigabitethernet 1/0/2
 shutdown
exit
interface gigabitethernet 1/0/3
 shutdown
exit
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
```

```
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
tunnel gre 1 #GRE tunnel number is reserved - it should not be changed
 mtu 1356 #do not specify - will be received from the SA (ipsec gre-mtu-offset)
 keepalive retries 3 #do not specify - will be received from the SA (ipsec gre-ping-counter)
 keepalive dst-address 10.2.0.1 #do not specify - will be received via DHCP in suboption 15 of option
43
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 keepalive enable #do not specify - GRE keepalive will be enabled automatically when received via
DHCP in suboption 15 of option 43
 mode ethernet
 local address xauth ipsec_vpn #the address will be received via mode-cfg when establishing IPsec
connection, the name IPsec VPN is reserved and cannot be changed
 remote address xauth ipsec_vpn management-ip #the address will be received via mode-cfg when
establishing IPsec connection, the name IPsec VPN is reserved and cannot be changed
 enable
exit
tunnel gre 1.1 #sub-GRE tunnel number is reserved and cannot be changed
 bridge-group 1
 mtu 1352 #do not specify - will be received from the SA (ipsec gre-mtu-offset)
 snmp init-trap
 enable
exit

security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
 rule 1
  action permit
  match source-address SoftWLC
  enable
 exit
exit

access profile acc_p #the name is reserved and cannot be changed
 user a8:f9:4b:ab:81:20 #do not specify - will be received from the SA (ipsec xauth-user)
  password ascii-text encrypted 9FB30B49E43D47FAC32E0994C89C75B81313F0F038CC02FC #do not
```

specify - will be received from the SA (ipsec xauth-password)
 exit
exit

security ike proposal ike_prop #the name is reserved and cannot be changed
 authentication algorithm md5 #do not specify - will be received from the SA (ipsec auth-alg)
 encryption algorithm aes128 #do not specify - will be received from the SA (ipsec encrypt-alg)
 dh-group 1 #do not specify - will be received from the SA (ipsec dh-group)
exit

security ike policy ike_pol #the name is reserved and cannot be changed
 lifetime seconds 86400 #do not specify - will be received from the SA (ipsec lifetime)
 pre-shared-key ascii-text testing123 #do not specify - will be received from the SA (ipsec password)
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw #the name is reserved and cannot be changed
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote address 100.64.0.1 #do not specify - will be received from the SA (ipsec remote-gateway)
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
 dead-peer-detection timeout 60 #will be received from the SA (ipsec dpd-delay)
 xauth access-profile acc_p client a8:f9:4b:ab:81:20 #do not specify - will be generated on the base of xauth-user received from the SA
exit

security ipsec proposal ipsec_prop #the name is reserved and cannot be changed
 authentication algorithm md5 #do not specify - will be received from the SA (ipsec sa-auth-alg)
 encryption algorithm aes128 #do not specify - will be received from the SA (ipsec sa-encrypt-alg)
exit

security ipsec policy ipsec_pol #the name is reserved and cannot be changed
 lifetime seconds 3600 #do not specify - will be received from the SA (ipsec sa-lifetime)
 proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn #the name is reserved and cannot be changed

 mode ike
 ike establish-tunnel immediate

```
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

ip ssh server
```

Finally, the following configuration will be obtained and written to custom-config

**Configuration in custom-config**

```
hostname ESR10-OTT

object-group network SoftWLC
 ip address-range 100.123.0.2
exit

syslog console debug
syslog monitor info

line console

 aaa disable

exit


security zone trusted
exit
security zone untrusted
exit

snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 100.123.0.2

source-interface bridge 1
exit



snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
```

*snmp-server enable traps environment cpu-load*
*snmp-server enable traps environment cpu-critical-temp*
*snmp-server enable traps environment cpu-overheat-temp*
*snmp-server enable traps environment cpu-supercooling-temp*
*snmp-server enable traps file-operations*
*snmp-server enable traps file-operations successful*
*snmp-server enable traps file-operations failed*
*snmp-server enable traps file-operations canceled*
*snmp-server enable traps interfaces*
*snmp-server enable traps interfaces rx-utilization-high*
*snmp-server enable traps interfaces tx-utilization-high*
*snmp-server enable traps interfaces number-high*
*snmp-server enable traps bras*
*snmp-server enable traps bras sessions-number-high*
*snmp-server enable traps screen*
*snmp-server enable traps screen dest-limit*
*snmp-server enable traps screen source-limit*
*snmp-server enable traps screen icmp-threshold*
*snmp-server enable traps screen udp-threshold*
*snmp-server enable traps screen syn-flood*
*snmp-server enable traps screen land*
*snmp-server enable traps screen winnuke*
*snmp-server enable traps screen icmp-frag*
*snmp-server enable traps screen udp-frag*
*snmp-server enable traps screen icmp-large*
*snmp-server enable traps screen syn-frag*
*snmp-server enable traps screen unknown-proto*
*snmp-server enable traps screen ip-frag*
*snmp-server enable traps screen port-scan*
*snmp-server enable traps screen ip-sweep*
*snmp-server enable traps screen syn-fin*
*snmp-server enable traps screen fin-no-ack*
*snmp-server enable traps screen no-flag*
*snmp-server enable traps screen spoofing*
*snmp-server enable traps screen reserved*
*snmp-server enable traps screen quench*
*snmp-server enable traps screen echo-request*
*snmp-server enable traps screen time-exceeded*
*snmp-server enable traps screen unreachable*
*snmp-server enable traps screen tcp-all-flags*
*snmp-server enable traps entity*
*snmp-server enable traps entity config-change*
*snmp-server enable traps entity-sensor*
*snmp-server enable traps entity-sensor threshold*
*snmp-server enable traps envmon*
*snmp-server enable traps envmon shutdown*
*snmp-server enable traps envmon temperature*
*snmp-server enable traps flash*

```
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart
snmp-server enable traps snmp linkdown
snmp-server enable traps snmp linkup
snmp-server enable traps syslog

bridge 1
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore router
 enable
exit

interface gigabitethernet 1/0/1
 description "UPLink"
 ip address dhcp
 security-zone untrusted
 service-policy dynamic all
exit
interface gigabitethernet 1/0/2
 shutdown
exit
interface gigabitethernet 1/0/3
 shutdown
exit
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
tunnel gre 1
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 mode ethernet
 local address xauth ipsec_vpn
 remote address xauth ipsec_vpn management-ip
 enable
exit
tunnel gre 1.1
```

```
 bridge-group 1
 snmp init-trap
 enable
exit

security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
 rule 1
  action permit
  match source-address SoftWLC
  enable
 exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
exit

security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
  proposal ipsec_prop
exit
```

```
security ipsec vpn ipsec_vpn
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

ip ssh server
```

Configuration for client connection

Default part of the configuration used for OTT installation remains the same. A client termination interface (bridge) on which BRAS works is added to it. Tagged traffic from SSID is received via subinterfaces that are grouped into a client bridge. To do that, any interfaces including uplink ones can be used. Untagged traffic from SSID can be received via ports gi1/0/2-6 (uplink gi1/0/1 should not be used for this purpose). To tag traffic in access mode, the same vlan as in bridge settings is used. Clients access the Internet using NAT via a current uplink address.
Configuration in which Internet access is provided via gi1/0/1, traffic from SSID1 and SSID1 comes to the same port with the tags 2314 and 2315 respectively. Both vlans are grouped into one client bridge 11 using subinterfaces. Clients access the Internet via NAT using the uplink gi1/0/1.

**Configuration**

```
hostname ESR10-OTT-BR-1

ip firewall sessions classification enable
object-group service dns
  port-range 53
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service redirect
port-range 3128-3129
port-range 3130-3131
exit

object-group network natpool
  ip prefix 198.19.253.0/24
exit
object-group network SoftWLC
 ip address-range 192.168.42.178
exit
```

```
radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
 key ascii-text encrypted 88B11079B9014FAAF7B9
 timeout 11
 priority 20
 source-interface bridge 1
 auth-port 31812
 acct-port 31813
 retransmit 10
 dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 192.168.42.178
exit
das-server COA
 key ascii-text encrypted 88B11079B9014FAAF7B9
 port 3799
 clients object-group SoftWLC
exit
aaa das-profile COA
 das-server COA
exit

line console
 aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
 rule 1
  action permit
  match protocol tcp
  match destination-port 443
  enable
 exit
 rule 2
  action permit
  match protocol tcp
  match destination-port 8443
  enable
 exit
```

```
 rule 3
  action permit
  match protocol tcp
  match destination-port 80
  enable
 exit
 rule 4
  action permit
  match protocol tcp
  match destination-port 8080
  enable
 exit
exit

ip access-list extended INTERNET
 rule 1
  action permit
  enable
 exit
exit

ip access-list extended unauthUSER
 rule 1
  action permit
  match protocol udp
  match source-port 68
  match destination-port 67
  enable
 exit
 rule 2
  action permit
  match protocol udp
  match destination-port 53
  enable
 exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
 aaa das-profile COA
 aaa sessions-radius-profile PCRF
 aaa services-radius-profile PCRF
 nas-interface bridge 1
 session mac-authentication
 bypass-traffic-acl unauthUSER
 default-service
  class-map unauthUSER
  filter-name remote gosuslugi
  filter-action permit
  default-action redirect http://192.168.42.178:8080/eltex_portal/
```

```
  session-timeout 600
 exit
 enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
 source-interface bridge 1
exit

snmp-server enable traps
snmp-server enable traps config
snmp-server enable traps config commit
snmp-server enable traps config confirm
snmp-server enable traps environment
snmp-server enable traps environment memory-flash-critical-low
snmp-server enable traps environment memory-flash-low
snmp-server enable traps environment memory-ram-critical-low
snmp-server enable traps environment memory-ram-low
snmp-server enable traps environment cpu-load
snmp-server enable traps environment cpu-critical-temp
snmp-server enable traps environment cpu-overheat-temp
snmp-server enable traps environment cpu-supercooling-temp
snmp-server enable traps file-operations
snmp-server enable traps file-operations successful
snmp-server enable traps file-operations failed
snmp-server enable traps file-operations canceled
snmp-server enable traps interfaces
snmp-server enable traps interfaces rx-utilization-high
snmp-server enable traps interfaces tx-utilization-high
snmp-server enable traps interfaces number-high
snmp-server enable traps bras
snmp-server enable traps bras sessions-number-high
snmp-server enable traps screen
snmp-server enable traps screen dest-limit
snmp-server enable traps screen source-limit
snmp-server enable traps screen icmp-threshold
snmp-server enable traps screen udp-threshold
snmp-server enable traps screen syn-flood
snmp-server enable traps screen land
snmp-server enable traps screen winnuke
snmp-server enable traps screen icmp-frag
snmp-server enable traps screen udp-frag
snmp-server enable traps screen icmp-large
snmp-server enable traps screen syn-frag
snmp-server enable traps screen unknown-proto
```

```
snmp-server enable traps screen ip-frag
snmp-server enable traps screen port-scan
snmp-server enable traps screen ip-sweep
snmp-server enable traps screen syn-fin
snmp-server enable traps screen fin-no-ack
snmp-server enable traps screen no-flag
snmp-server enable traps screen spoofing
snmp-server enable traps screen reserved
snmp-server enable traps screen quench
snmp-server enable traps screen echo-request
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart

bridge 1
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore dns-nameserver
 ip dhcp client ignore router
 enable
exit
bridge 11
 security-zone user
 ip address 198.19.253.1/24
 service-subscriber-control any
 location SSID12
 enable
exit

interface gigabitethernet 1/0/1
 description "UPLink"
 ip address dhcp
 security-zone untrusted
 service-policy dynamic all
exit
interface gigabitethernet 1/0/1.2314
```

```
 bridge-group 11
exit
interface gigabitethernet 1/0/1.2315
 bridge-group 11
exit
interface gigabitethernet 1/0/2
 shutdown
exit
interface gigabitethernet 1/0/3
 shutdown
exit
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
tunnel gre 1
 keepalive retries 3
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 mode ethernet
 local address xauth ipsec_vpn
 remote address xauth ipsec_vpn management-ip
 enable
exit
tunnel gre 1.1
 bridge-group 1
 snmp init-trap
 enable
exit
security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
  rule 1
   action permit
  enable
 exit
```

```
exit
security zone-pair user untrusted
 rule 10
  action permit
  enable
 exit
exit
security zone-pair user self
 rule 10
  action permit
  match protocol udp
  match source-port dhcp_client
  match destination-port dhcp_server
  enable
 exit
 rule 20
  action permit
  match protocol tcp
  match destination-port redirect
  enable
 exit
 rule 30
  action permit
  match protocol udp
  match destination-port dns
  enable
 exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
exit
```

```
security ipsec proposal ipsec_prop
exit

security ipsec policy ipsec_pol
 proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

nat source
 ruleset NAT
  to interface gigabitethernet 1/0/1
  rule 10
   match source-address natpool
   action source-nat interface

   enable
  exit
 exit
exit

ip dhcp-server
 ip dhcp-server pool lan
 network 198.19.253.0/24
 max-lease-time 000:00:20
 default-lease-time 000:00:10
 address-range 198.19.253.2-198.19.253.254
 default-router 198.19.253.1
 dns-server 198.19.253.1
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 192.168.42.178
exit
```

Configuration in which uplink is connected via gi1/0/1, and access points are connected via gi1/0/2 - tagged traffic with the tag 701; gi1/0/3 - untagged traffic that will be tagged with 701.

**Configuration**

```
hostname ESR10-OTT-BR

ip firewall sessions classification enable
```

```
root login enable
tech-support login enable
object-group service dns
 port-range 53
exit
object-group service dhcp_server
 port-range 67
exit
object-group service dhcp_client
 port-range 68
exit
object-group service redirect
 port-range 3128-3129
 port-range 3130-3131
exit

object-group network natpool
 ip prefix 198.19.253.0/24
exit
object-group network SoftWLC
 ip address-range 192.168.42.178
exit

vlan 701
exit

radius-server timeout 10
radius-server retransmit 5
radius-server host 192.168.42.178
 key ascii-text encrypted 88B11079B9014FAAF7B9
 timeout 11
 priority 20
 source-interface bridge 1
 auth-port 31812
 acct-port 31813
 retransmit 10
 dead-interval 10
exit
aaa radius-profile PCRF
 radius-server host 192.168.42.178
exit
das-server COA
 key ascii-text encrypted 88B11079B9014FAAF7B9
 port 3799
 clients object-group SoftWLC
exit
```

```
aaa das-profile COA
 das-server COA
exit

line console
 aaa disable
exit

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone user
exit

ip access-list extended WELCOME
 rule 1
  action permit
  match protocol tcp
  match destination-port 443
  enable
 exit
 rule 2
  action permit
  match protocol tcp
  match destination-port 8443
  enable
 exit
 rule 3
  action permit
  match protocol tcp
  match destination-port 80
  enable
 exit
 rule 4
  action permit
  match protocol tcp
  match destination-port 8080
  enable
 exit
exit
ip access-list extended INTERNET
 rule 1
  action permit
```

```
   enable
  exit
exit

ip access-list extended unauthUSER
  rule 1
   action permit
   match protocol udp
   match source-port 68
   match destination-port 67
   enable
  exit
  rule 2
   action permit
   match protocol udp
   match destination-port 53
   enable
  exit
exit

subscriber-control filters-server-url http://192.168.42.178:7070/filters/file
subscriber-control
  aaa das-profile COA
  aaa sessions-radius-profile PCRF
  aaa services-radius-profile PCRF
  nas-interface bridge 1
  session mac-authentication
  bypass-traffic-acl unauthUSER
  default-service
   class-map unauthUSER
   filter-name remote gosuslugi
   filter-action permit
   default-action redirect http://192.168.42.178:8080/eltex_portal/
   session-timeout 600
  exit
  enable
exit
snmp-server
snmp-server system-shutdown
snmp-server community "public11" ro
snmp-server community "private1" rw

snmp-server host 192.168.42.178
  source-interface bridge 1
exit
```

*snmp-server enable traps*
*snmp-server enable traps config*
*snmp-server enable traps config commit*
*snmp-server enable traps config confirm*
*snmp-server enable traps environment*
*snmp-server enable traps environment memory-flash-critical-low*
*snmp-server enable traps environment memory-flash-low*
*snmp-server enable traps environment memory-ram-critical-low*
*snmp-server enable traps environment memory-ram-low*
*snmp-server enable traps environment cpu-load*
*snmp-server enable traps environment cpu-critical-temp*
*snmp-server enable traps environment cpu-overheat-temp*
*snmp-server enable traps environment cpu-supercooling-temp*
*snmp-server enable traps file-operations*
*snmp-server enable traps file-operations successful*
*snmp-server enable traps file-operations failed*
*snmp-server enable traps file-operations canceled*
*snmp-server enable traps interfaces*
*snmp-server enable traps interfaces rx-utilization-high*
*snmp-server enable traps interfaces tx-utilization-high*
*snmp-server enable traps interfaces number-high*
*snmp-server enable traps bras*
*snmp-server enable traps bras sessions-number-high*
*snmp-server enable traps screen*
*snmp-server enable traps screen dest-limit*
*snmp-server enable traps screen source-limit*
*snmp-server enable traps screen icmp-threshold*
*snmp-server enable traps screen udp-threshold*
*snmp-server enable traps screen syn-flood*
*snmp-server enable traps screen land*
*snmp-server enable traps screen winnuke*
*snmp-server enable traps screen icmp-frag*
*snmp-server enable traps screen udp-frag*
*snmp-server enable traps screen icmp-large*
*snmp-server enable traps screen syn-frag*
*snmp-server enable traps screen unknown-proto*
*snmp-server enable traps screen ip-frag*
*snmp-server enable traps screen port-scan*
*snmp-server enable traps screen ip-sweep*
*snmp-server enable traps screen syn-fin*
*snmp-server enable traps screen fin-no-ack*
*snmp-server enable traps screen no-flag*
*snmp-server enable traps screen spoofing*
*snmp-server enable traps screen reserved*
*snmp-server enable traps screen quench*
*snmp-server enable traps screen echo-request*

```
snmp-server enable traps screen time-exceeded
snmp-server enable traps screen unreachable
snmp-server enable traps screen tcp-all-flags
snmp-server enable traps entity
snmp-server enable traps entity config-change
snmp-server enable traps entity-sensor
snmp-server enable traps entity-sensor threshold
snmp-server enable traps envmon
snmp-server enable traps envmon shutdown
snmp-server enable traps envmon temperature
snmp-server enable traps flash
snmp-server enable traps flash insertion
snmp-server enable traps flash removal
snmp-server enable traps snmp
snmp-server enable traps snmp authentication
snmp-server enable traps snmp coldstart

bridge 1
 security-zone trusted
 ip address dhcp
 ip dhcp client ignore dns-nameserver
 ip dhcp client ignore router
 enable
exit
bridge 2
 vlan 701
 security-zone user
 ip address 198.19.253.1/24
 service-subscriber-control any
 location SSID12
 enable
exit

interface gigabitethernet 1/0/1
 description "UPLink"
 ip address dhcp
 security-zone untrusted
 service-policy dynamic all
exit
interface gigabitethernet 1/0/2.702
 bridge-group 2
exit
interface gigabitethernet 1/0/3
 mode switchport
 switchport access vlan 701
exit
```

```
interface gigabitethernet 1/0/4
 shutdown
exit
interface gigabitethernet 1/0/5
 shutdown
exit
interface gigabitethernet 1/0/6
 shutdown
exit
interface loopback 1
exit
tunnel gre 1
 keepalive retries 3
 keepalive dhcp dependent-interface bridge 1
 keepalive dhcp dependent-interface gi1/0/1
 mode ethernet
 local address xauth ipsec_vpn
 remote address xauth ipsec_vpn management-ip
 enable
exit
tunnel gre 1.1
 bridge-group 1
 snmp init-trap
 enable
exit

security zone-pair untrusted self
 rule 1
  action permit
  match protocol icmp
  enable
 exit
exit
security zone-pair trusted self
 rule 1
  action permit
  enable
 exit
exit
security zone-pair user untrusted
 rule 10
  action permit
  enable
 exit
exit
security zone-pair user self
```

```
 rule 10
  action permit
  match protocol udp
  match source-port dhcp_client
  match destination-port dhcp_server
  enable
 exit
 rule 20
  action permit
  match protocol tcp
  match destination-port redirect
  enable
 exit
 rule 30
  action permit
  match protocol udp
  match destination-port dns
  enable
 exit
exit

access profile acc_p
exit

security ike proposal ike_prop
exit

security ike policy ike_pol
 authentication method xauth-psk-key
 authentication mode client
 proposal ike_prop
exit

security ike gateway ike_gw
 ike-policy ike_pol
 assign-interface loopback 1
 local interface gigabitethernet 1/0/1
 remote network dynamic client
 mode policy-based
 dead-peer-detection action restart
 dead-peer-detection interval 10
 dead-peer-detection timeout 60
exit

security ipsec proposal ipsec_prop
exit
```

```
security ipsec policy ipsec_pol
 proposal ipsec_prop
exit

security ipsec vpn ipsec_vpn
 mode ike
 ike establish-tunnel immediate
 ike gateway ike_gw
 ike ipsec-policy ipsec_pol
 enable
exit

nat source
 ruleset NAT
  to interface gigabitethernet 1/0/1
  rule 10
   match source-address natpool
   action source-nat interface
   enable
  exit
 exit
exit

ip dhcp-server
ip dhcp-server pool lan
 network 198.19.253.0/24
 max-lease-time 000:00:20
 default-lease-time 000:00:10
 address-range 198.19.253.2-198.19.253.254
 default-router 198.19.253.1
 dns-server 198.19.253.1
exit

ip telnet server
ip ssh server

clock timezone gmt +7

ntp enable
ntp server 192.168.42.178
exit
```

List of error codes sent by ESR-10 to the Service Activator

If a connection error occurs, ESR-10 will reset to factory configuration and send and error code to the SA. After 5 minutes or after expiry of wait-timer, if it has been received, connect to the SA again.

| error code | description |
|---|---|
| 0 | Error in application of configuration received from the SA |
| 3 | Incorrect IPsec parameters in case if some IPsec parameters are empty |
| 16 | Suboption 15 of option 43 containing an address for GRE keepalive has not been received on the management interface during wait timer |
| 17 | Empty data in the section "OTT custom config" of the SA response |

## v1.14_MySQL (EN)


- Service management
- Configuration
  - The number of connections
  - Memory size
  - Collecting rsyslog
  - Checking replication ststus in GUI EMS
- Database connection number calculation depending on server load
- mysql server operation analysis using MySQLTuner


# Description

MySQL is a relational database used in SoftWLC project to store key data required for the management system operation. The version **mysql-server-5.5** is used.
The project includes the following databases:

| Database | Description |
|---|---|
| **eltex_ems** | contains data on domain structure, object tree, EMS users, EMS configuration data etc. The database is created/updated when eltex-ems-db package is installed. |
| **eltex_alert** | contains EMS and device event logs. The database is created/updated when eltex-ems-db package is installed. |
| **wireless** | contains SSID configuration. The database is created/updated when eltex-ems-db package is installed. |
| **eltex_auth_service** | the database used by eltex-auth-service package to store data on Admin Panel, Portal Constructor and NBI users. The database is created/updated during eltex-auth-service-db package installation. |
| **radius** | contains data on Wi-Fi users, their usernames, customization and accounting. The database is created/updated during freeradius-eltex-db package installation. |

| | |
|---|---|
| **ELTEX_PORTAL** | contains data on virtual portals used in the project. The database is created/updated during eltex-portal-mysql package installation. |
| **payments** | contains data on Wi-Fi users' payments for using paid tariffs. The database is created/updated during eltex-portal-mysql package installation. |
| **eltex_doors** | contains JWT tokens generated by eltex-doors service. |

## Service management

| Operation | Command | Response |
|---|---|---|
| Status check | `service mysql status` | Service is running<br>`mysql start/running, process <pid>`<br><br>Service is waiting<br>`mysql stop/waiting` |
| Service start | `service mysql start` | Service has been started<br>`mysql start/running, process <pid>`<br><br>The service is already running<br>`start: Job is already running: mysql` |
| Service stop | `service mysql stop` | Service has been stopped successfully<br>`mysql stop/waiting` |
| Service restart | `service mysql restart` | Service has been restarted successfully<br>`mysql stop/waiting mysql start/ running, process <pid>` |

## Configuration

MySQL configuration is done via **/etc/mysql/my.cnf** (default file installed with mysql-server package) and **/etc/mysql/conf.d/eltex-ems.cnf** (the file installed with eltex-ems-db package and containing additional information which is important for the management system work) configuration files.

### The number of connections

Depending on the estimated number of access points, the maximum number of AP connections should be specified via **max_connections** parameter. The parameter is specified in **/etc/mysql/mysql.conf.d/mysql.cnf** by default, but commented out. Uncomment it and enter the required number, for example, like this:

```
max_connections        = 500
```

The number can be selected from **Calculating the number of database connections depending on server load** (last row).

### Memory size

MyISAM is used in eltex_alert database and syslog. InnoDB is used in all other databases, including radius.radacct high-load table.
After the database is installed, configure buffer size for MyISAM and InnoDB services (**/etc/mysql/conf.d/eltex-ems.cnf** parameters **key_buffer_size** and **innodb_buffer_pool_size**, respectively).Configuration recommendations:

- If the database is installed on a dedicated host, the recommended buffer size is 30-40% of total RAM for each service.
- If all the services are installed on the same host, buffer size available for each service is calculated assuming that the main Java application (eltex-ems), tomcat7 web server, NBI, Admin Panel and eltex-apb also require big virtual memory size. They should be specified for each service in relevant configuration files.
- Memory size available for InnoDB may be 2-3 times bigger then one for MyISAM, if there are no plans to collect syslog from many devices.

For example, if all SoftWLC services are installed on the same host, the following amounts of memory are allocated:
For 16G server:

```
key_buffer_size = 2G
innodb_buffer_pool_size = 4G
```

For 64G server:

```
key_buffer_size=8G
innodb_buffer_pool_size=24G
```

When /etc/mysql/conf.d/eltex-ems.cnf configuration file is modified, restart MySQL with the command:

```
service mysql restart
```

**key_buffer_size and innodb_buffer_pool_size parameters can be changed at any time according to machine perfomance. The changes do not have an impact on processing speed during MySQL service operation and cannot lead to loss of saved data or to file system structure changes.**

# Additional database user accounts

## Collecting rsyslog

To collect logs from DHCP and RADIUS servers, rsyslog user account should be created in the database. Commands:

```
CREATE USER 'rsyslog'@'HOST' identified by 'root';
GRANT ALL on Syslog.* TO 'rsyslog'@'HOST' identified by 'root';
```

where **HOST** is an address of RADIUS or DHCP server in management network. For each server, a separate entry should be created.

## Checking replication ststus in GUI EMS

For EMS server to be able to check replication state, additional user accounts are required. They can be created via the MySQL console:
commands:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'HOST' IDENTIFIED BY 'root';
FLUSH PRIVILEGES;
```

where **HOST** is an address of EMS server in VRRP network. For each server, a separate entry should be created.

## Database connection number calculation depending on server load

| | | up to 50 AP | from 50 to 200 AP | from 200 to 500 AP | from 500 to 4 thousand AP |
|---|---|---|---|---|---|
| The number of SoftWLC service connections (these settings are specified in services' configuration files for database connection) | | | | | |
| nbi (total) | | 16 | 38 | 78 | 156 |
| The number of service connections per DB | radius | 4 | 12 | 24 | 48 |
| | ems | 4 | 10 | 22 | 48 |
| | wireless | 4 | 10 | 22 | 48 |
| | logs | 2 | 4 | 6 | 8 |
| | eltex_auth_service | 2 | 2 | 4 | 4 |
| | | | | | |
| ems (total) | | 20 | 40 | 92 | 186 |
| The number of service connections per DB | event | 4 | 8 | 16 | 32 |
| | tree | 4 | 8 | 20 | 40 |
| | syslog | 2 | 4 | 4 | 4 |
| | radius | 4 | 8 | 20 | 40 |
| | wireless | 3 | 6 | 14 | 30 |
| | | | | | |
| PCRF (total) | | 6 | 12 | 24 | 48 |
| The number of service connections per DB | radius | 2 | 4 | 8 | 16 |
| | sql.ems | 2 | 4 | 8 | 16 |

| | | | | | |
|---|---|---|---|---|---|
| | sql.wireless | 2 | 4 | 8 | 16 |
| | | | | | |
| radius | | 5 | 10 | 15 | 32 |
| eltex-auth | | 2 | 2 | 2 | 5 |
| eltex-portal | | 10 | 10 | 15 | 32 |
| eltex-portal-constructor | | 10 | 10 | 10 | 10 |
| rsyslog-mysql | | 2 | 4 | 6 | 10 |
| | | | | | |
| replication | | 2 | 2 | 2 | 2 |
| reserve | | 8 | 8 | 8 | 8 |
| | | | | | |
| The total number of MySQL connections<br>(the number of connections that should be specified in the database configuration) | | 78 | 130 | 234 | 449 |

## mysql server operation analysis using MySQLTuner

MySQLTuner is a perl script that analyses MySQL statistics and provides recommendations on MySQL server configuration optimization.

**Note! MySQL server should operate without reloadings and configuration parameters changes for some period of time (at least 24 hours according to MysqTuner).**

To start the script, run the command:

```
/usr/lib/eltex-ems-db/tools/mysqltuner.pl -- user root --pass root
```

When started, the script will conduct an analysis and give the following information:

```
>> MySQLTuner 1.2.0 - Major Hayden <major@mhtx.net>
>> Bug reports, feature requests, and downloads at http://mysqltuner.com/
>> Run with '--help' for additional options and output filtering
[OK] Logged in using credentials from debian maintenance account.
-------- General Statistics --------------------------------------------------
[--] Skipped version check for MySQLTuner script
[OK] Currently running supported MySQL version 5.5.43-0ubuntu0.14.04.1-log
[OK] Operating on 64-bit architecture

-------- Storage Engine Statistics -------------------------------------------
[--] Status: +Archive BDB -Federated +InnoDB -ISAM -NDBCluster
[-] Data in PERFORMANCE_SCHEMA tables: 0B (Tables: 17)
[--] Data in InnoDB tables: 3G (Tables: 39)
[--] Data in MyISAM tables: 22G (Tables: 5)
[!!] Total fragmented tables: 10

-------- Security Recommendations -------------------------------------------
[OK] All database users have passwords assigned

-------- Performance Metrics -------------------------------------------------
[--] Up for: 127d 22h 20m 14s (746M q [67.539 qps], 25M conn, TX: 302B, RX: 411B)
[--] Reads / Writes: 21% / 79%
[--] Total buffers: 48.1G global + 2.7M per thread (151 max threads)
[OK] Maximum possible memory usage: 48.5G (77% of installed RAM)
[OK] Slow queries: 0% (13K/746M)
[!!] Highest connection usage: 100% (152/151)
[OK] Key buffer size / total MyISAM indexes: 24.0G/9.9G
[OK] Key buffer hit rate: 99.9% (4B cached / 5M reads)
[OK] Query cache efficiency: 33.6% (114M cached / 340M selects)
[!!] Query cache prunes per day: 735211
[OK] Sorts requiring temporary tables: 0% (1K temp sorts / 5M sorts)
[OK] Temporary tables created on disk: 0% (3K on disk / 394K total)
[OK] Thread cache hit rate: 99% (8K created / 25M connections)
[!!] Table cache hit rate: 8% (324 open / 3K opened)
[OK] Open file limit used: 19% (3K/16K)
[OK] Table locks acquired immediately: 99% (9B immediate / 9B locks)
[OK] InnoDB data size / buffer pool: 3.6G/24.0G

-------- Recommendations -----------------------------------------------------
General recommendations:
Run OPTIMIZE TABLE to defragment tables for better performance
Enable the slow query log to troubleshoot bad queries
Reduce or eliminate persistent connections to reduce connection usage
Increase table_cache gradually to avoid file descriptor limits
Variables to adjust:
max_connections (> 151)
wait_timeout (< 28800)
interactive_timeout (< 28800)
query_cache_size (> 16M)
```

```
table_cache (> 400)
```

⚠ Special attention should be paid to the lines marked with [!!], "Maximum possible memory usage" parameter (its value should be less than total RAM size) and Recommendations section.

## v1.14_Configuring MySQL replication

Reservation of data stored in MySQL tables is carried out by master-master replication. According to that, all database updates made on the first host are transmitted to the second one in real time. Thus, each copy of Eltex.EMS service has the same virtual address as one of database management system's copies (http://dev.mysql.com/doc/refman/5.5/en/replication.html). That allows having a relevant copy of a database on two hosts simultaneously. If connection is failed, changes are accumulated and then synchronized after reconnection.

### 1. Replication configuration

Make the following changes in **[ mysqld ]** section of **/etc/mysql/my.cnf** configuration file:

Comment out or delete the line:

```
bind-address = 127.0.0.1
```

Specify server-id. The servers should be assigned different identifiers, e.g. for the first server:

```
server-id = 1
```

for the second server:

```
server-id = 2
```

Enable binary logs:

```
log_bin = /var/log/mysql/mysql-bin.log;
```

specify **auto_increment_increment** (increment step) and **auto_increment_offset** (start point) parameters.

For the first server:

```
auto_increment_increment= 2
```

```
auto_increment_offset = 1
```

For the second server:

```
auto_increment_increment= 2

auto_increment_offset = 2
```

Specify databases for which logs will be generated:

```
binlog-do-db = eltex_alert

binlog-do-db = eltex_ems

binlog-do-db = wireless binlog-do-db = radius

binlog-do-db = eltex_auth_service

binlog-do-db = ELTEX_PORTAL

binlog-do-db = payments
```

Specify databases for which logs will not be generated:

```
binlog-ignore-db = mysql

binlog-ignore-db = Syslog

binlog-ignore-db = performance_schema

binlog-ignore-db = information_schema
```

Restart **mysql** service on each server and create a database for replication.

**2. Creating accounts for replication**

Create an account for replication on the first server:

```
GRANT REPLICATION SLAVE ON *.* TO 'replication'@'<ip_server2>' IDENTIFIED BY
'password';
FLUSH PRIVILEGES;
```

Create an account for replication on the second server:

```
GRANT REPLICATION SLAVE ON *.* TO 'replication'@'<ip_server1>' IDENTIFIED BY
'password';
FLUSH PRIVILEGES;
```

**3. Starting slave replication on the second server**

3.1 Run the **show master status** command in MySQL console of the **first** server and analyze values obtained:

```
show master status \G
```

The reply should be as follows:

```
mysql> show master status \G
*************************** 1. row ***************************
            File: mysql-bin.000001
        Position: 00000107
    Binlog_Do_DB:
eltex_alert,eltex_ems,eltex_ont,radius,wireless,eltex_auth_service,payments,ELTE
X_PORTAL
Binlog_Ignore_DB: mysql,Syslog,performance_schema,information_schema
1 row in set (0.00 sec)
```

Copy the paramaters **File** and **Position** parameters.

3.2 Configure and start the **second** server replication from the first one **(perform the following operations on the second server):**

```
mysql>  CHANGE MASTER TO MASTER_HOST='<ip_server1>', MASTER_USER='replication',
MASTER_PASSWORD='password', MASTER_LOG_FILE='mysql-bin.000001',
MASTER_LOG_POS=107;
START SLAVE;
```

**where**
MASTER_LOG_FILE=**'mysql-bin.000001'** – specify the **File** value obtained in the previous paragraph.
MASTER_LOG_POS=**107** – specify the **Position** value obtained in the previous paragraph.

3.3 Check replication state:

```
mysql> show slave status \G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: <ip_server1>
                  Master_User: replication
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.001783
          Read_Master_Log_Pos: 107
               Relay_Log_File: mysqld-relay-bin.000001
                Relay_Log_Pos: 107
        Relay_Master_Log_File: mysql-bin.001783
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
```

```
  Replicate_Wild_Ignore_Table:
                  Last_Errno: 0
                  Last_Error:
                Skip_Counter: 0
         Exec_Master_Log_Pos: 107
             Relay_Log_Space: 107
             Until_Condition: None
              Until_Log_File:
               Until_Log_Pos: 0
          Master_SSL_Allowed: No
          Master_SSL_CA_File:
          Master_SSL_CA_Path:
             Master_SSL_Cert:
           Master_SSL_Cipher:
              Master_SSL_Key:
        Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 0
                Last_IO_Error:
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 2
1 row in set (0.00 sec)
```

If ***Slave _ IO _ Running*** **and** ***Slave _ SQL _ Running*** parameters are set to *« **Yes** »,* replication has been launched successfully.

3.4 Create a table in the database on the first server and add data to it or create a dump.

```
use eltex_ems;
create table test1 (mid int(11) auto_increment, PRIMARY KEY (mid))
Engine=MyISAM;
```

3.4 On the second server, check if the new table has been copied.

**4. Starting replication on the first server**

4.1 Run **show master status** command on the second server:

```
show master status \G
```

The reply should be as follows:

```
mysql> show master status \G
*************************** 1. row ***************************
            File: mysql-bin.000001
        Position: 00000107
    Binlog_Do_DB:
eltex_alert,eltex_ems,eltex_ont,radius,wireless,eltex_auth_service,payments,ELTE
X_PORTAL
Binlog_Ignore_DB: mysql,Syslog,performance_schema,information_schema
1 row in set (0.00 sec)
```

4.2 Configure and start the first server replication from the second one:

```
CHANGE MASTER TO MASTER_HOST='<ip_server2>', MASTER_USER='replication',
MASTER_PASSWORD='password', MASTER_LOG_FILE='mysql-bin.000001',
MASTER_LOG_POS=107;
START SLAVE;
```

4.3 Check replication state:

```
mysql> show slave status \G
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: <ip_server2>
                  Master_User: replication
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000001
          Read_Master_Log_Pos: 107
               Relay_Log_File: mysqld-relay-bin.000001
                Relay_Log_Pos: 107
        Relay_Master_Log_File: mysql-bin.000001
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
```

(the output given is incomplete, since other data is less important)
If the values are correct, replication is performed in either direction. Then the database should be filled with real data.

**5. The script to start replication on the servers**

Instead of adding all entries manually, the following script can be used:

```
#!/bin/bash
REMOTE_HOST='<opposite server's IP address>'
LOGIN='<login for root access to local and remote servers>'
PASS='<password for root access to local and remote servers>'

REMOTE_FILE=`mysql --host=$REMOTE_HOST --user=$LOGIN --password=$PASS -e "show master
status \G" | grep "File" | awk '{print $2}'`
REMOTE_POS=`mysql --host=$REMOTE_HOST --user=$LOGIN --password=$PASS -e "show master
status \G" | grep "Position" | awk '{print $2}'`

echo REMOTE_FILE=$REMOTE_FILE
echo REMOTE_POS=$REMOTE_POS
mysql --user=$LOGIN --password=$PASS -e "stop slave"
mysql --user=$LOGIN --password=$PASS -e "CHANGE MASTER TO MASTER_HOST='$REMOTE_HOST',
MASTER_USER='replication', MASTER_PASSWORD='password', MASTER_LOG_FILE='$REMOTE_FILE',
MASTER_LOG_POS=$REMOTE_POS;"
mysql --user=$LOGIN --password=$PASS -e "start slave"
```

For the script to work, identical values with remote and local root access should be created in mysql.

**Automatic replication restart in case of server communication failure**

Create **/etc/keepalived/revive_mysql_replication.sh** file with the following contents on both servers:

```
#!/bin/bash
LOCAL_FILE=`mysql --user=root --password=root -e "show slave status \G" | grep"
Master_Log_File" | awk ' {print $2}'`
REMOTE_FILE=`mysql --host=<opposite server's IP address> --user=root --password=root -e "
show master status \G" | grep "File" | awk '{print $2}'`

if [ $LOCAL_FILE != $REMOTE_FILE ]
 then
 mysql --user=root --password=root -e "stop slave"
 mysql --user=root --password=root -e "start slave"
fi
```

where

**host** = **172.16.110.3** – the address of the opposite server.

To make the script run every minute, add the following command to cron:

```
crontab -l | { cat; echo "*/1 * * * * /etc/keepalived/
revive_mysql_replication.sh"; } | crontab
```

Add users on the first server (specify opposite server's IP address):

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'<ip_server2>' IDENTIFIED BY 'root';
FLUSH PRIVILEGES;
```

And on the second server:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'<ip_server1>' IDENTIFIED BY 'root';
FLUSH PRIVILEGES;
```

## v1.14_Restoring replication

One of the many ways to restore a replication in case of mysql-bin log loss is to use Percona Xtrabackup utility.

The advantage of using this method is that it does not require a MASTER server stop. The only condition is having binary logging enabled.

1) Install Xtrabackup utility

```
root@vagrant-ubuntu-trusty-64-test1111:~# apt install percona-xtrabackup
```

2) Prepare data for copying and create a database backup
To do that, create a new directory and copy files to it

```
root@vagrant-ubuntu-trusty-64-test1111:~/mysql# innobackupex --user=root --password=root /home/
vagrant/mysql/
```

In the directory created, a new one with the current date will appear
3) When a backup is created, data is not yet ready for the restore. The logs to be restored may contain cancelled transactions. It is required to apply a change log to a data file

```
root@vagrant-ubuntu-trusty-64-test1111:~/mysql# innobackupex --user=root --password=root --apply-
log /home/vagrant/mysql/2018-10-03_08-07-34/
```

When a backup is ready, copy data files to a SLAVE server
4) On the SLAVE server, stop mysql service and copy data to mysql directory.

```
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# service mysql stop
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# mv /var/lib/mysql /var/lib/mysql.old
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# cp /home/vagrant/mysql/2018-10-03_08-07-34/ /var/
lib/mysql
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# chown -R mysql:mysql /var/lib/mysql
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# service mysql start
```

5) Open mysql console, get the binary log's location and name. After that, configure replication on the SLAVE server.

```
root@vagrant-ubuntu-trusty-64-test4444:~/mysql# cat /home/vagrant/mysql/2018-10-03_08-07-34/
xtrabackup_binlog_info
mysql-bin.002454    9311320
```

```
mysql>  STOP SLAVE;
mysql>  CHANGE MASTER TO MASTER_HOST='<ip_server1>', MASTER_USER='replication',
MASTER_PASSWORD='password', MASTER_LOG_FILE='mysql-bin.002454', MASTER_LOG_POS=9311320;
mysql>  START SLAVE;
```

Check if replication is working

```
mysql> SHOW SLAVE STATUS\G;
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host: <ip_server1>
                  Master_User: replication
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.002455
          Read_Master_Log_Pos: 89717415
               Relay_Log_File: mysqld-relay-bin.000004
                Relay_Log_Pos: 89717561
        Relay_Master_Log_File: mysql-bin.002455
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
```

## v1.14_NBI (EN)


- Description
- Starting/stopping procedure
- Configuration
    - /etc/eltex-radius-nbi/radius_nbi_config.txt
- Configuring hikari cp
- Command documentation

## Description

The SOAP-based interface provides connection between SoftWLC components. NBI is used to support the work of the following services: Admin Panel, Portal Constructor, PCRF. It also allows conducting integration with higher OSS/BSS and generating TLS autorization certificates.
To install NBI, deploy **eltex-axis** package and then **eltex-radius-nbi** package (follow the order to avoid problems with the service operation).

## Starting/stopping procedure

The interface works with tomcat (version 7 and higher), so no specific commands are needed.

## Configuration

### /etc/eltex-radius-nbi/radius_nbi_config.txt

the file contains parameters for connecting to SoftWLC services.

- Settings for **MySQL** database connection. Different parameters can be used for different databases (connection to **ELTEX_PORTAL** database should definitely be set in the end of the file). As an example, connection to **radius** database is considered:

```
# DB  radius(alias=radius)
radius.jdbc.driver=org.gjt.mm.mysql.Driver
radius.jdbc.dbUrl=jdbc:mysql://localhost/radius?
zeroDateTimeBehavior=convertToNull&useUnicode=true&characterEncoding=utf8&rel
axAutoCommit=true&connectTimeout=5000
radius.jdbc.username=javauser
radius.jdbc.password=javapassword
radius.jdbc.maxPoolSize=48
radius.jdbc.inUse=yes
```

- **northbound EMS** connection required to send commands to **eltex-ems** service:

```
# адрес ems-northbound
ems.nbi.host=127.0.0.1
ems.nbi.port=8080
ems.nbi.path=northbound
ems.nbi.protocol=http
```

- **SSH** connection to **eltex-auth-service** is needed to restart the service if NAS table is changed via Admin Panel.

```
# eltex_auth_service
auth.port=22
auth.host=127.0.0.1
auth.username=username
auth.password=password
```

- **SSH** connection to **eltex-radius** needed to restart the service if NAS table is changed.

```
# freeradius-domain-1
freeradius-domain-1.port=22
freeradius-domain-1.host=192.168.0.1
freeradius-domain-1.username=username
freeradius-domain-1.password=password
```

- tomcat address available for Admin Panel users. It is used to generate TLS certificates for users and to provide links to log files.

```
# tomcat url
tomcat.host=127.0.0.1
tomcat.port=8080
```

- Address for downloading user TLS certificates. This should be an address of a server available for external network users.

```
# tomcat url
tomcat.host=127.0.0.1
tomcat.port=8080
```

- Connection to **PCRF**:

```
# pcrf stuff
pcrf.enabled=true
pcrf.url=http://localhost:7070
pcrf.username=admin
pcrf.password=password
```

- Connection to **pcrf** database of MongoDB cluster:

```
# pcrf mongodb connector
pcrf.mongodb.enabled=true
pcrf.mongodb.uri=mongodb://localhost:27017/pcrf
```

- Connection to **wifi-customer-cab** database of MongoDB cluster:

```
# wifi-customer-cab mongodb connector
wificab.mongodb.enabled=true
wificab.mongodb.uri=mongodb://localhost:27017/wifi-customer-cab
```

- Settings for SORM2 database connection (Mongo):

```
# Eltex.SORM2.replicator MongoDB 'sorm2' connect
sorm2.mongodb.enabled=false
sorm2.mongodb.uri=mongodb://localhost:27017/sorm2
```

- Connection to SORM2 service:

```
# Eltex.SORM2.replicator host to use API
sorm2.enabled=false
sorm2.url=http://localhost:7071
sorm2.username=admin
sorm2.password=password
```

- SORM3 functionality activation. Verification of Name and Telephone number fields is enabled for an operator when working with Wi-Fi users' accounts. Name and Telephone number fields become compulsory.

```
#It enables records export to SORM3 while editing wifi users
sorm3.enabled=false
```

- Setting a timeout for statistics loading in Admin Panel. Timeout is set to 90000 ms by default.

```
# wifi-customer-cab request settings
wificab.timeout=90000
```

## Configuring hikari cp

hikari cp connection pool is used for interaction between eltex-radius-nbi and MySQL database.

```
Connection timeout;
connectionTimeout=15000
Access validation timeout should be shorter than connectionTimeout;
validationTimeout=3000
Idle timeout. It should be in the range from 10000 (10 seconds) to 600000
(600 seconds);
idleTimeout=30000
Minimum number of free connections in hikari cp.
minimumIdle=1
```

## Command documentation

Relevant command documentation can be found in eltex-radius-nbi package. It becomes accessible after the package is downloaded via http://localhost:8080/eltex-radius-nbi/asciidoc/
WSDL file is available on http://localhost:8080/axis2/services/RadiusNbiService?wsdl
(replace localhost with ip address of a server with NBI)

# v1.14_Notification GW (EN)


- Description
- Starting/stopping procedure
- Configuration
  - /etc/eltex-ngw/notification.properties
  - /etc/default/eltex-ngw
  - Configuration files to connect SMS gateways


## Description

The service is an interface that provides interaction between platform components and external SMS gateways, call centers and e-mail servers. Notification GW is used to send notifications to platform and Wi-Fi users.

To install the service, use the package **eltex-ngw**.

## Starting/stopping procedure

To stop the service, the following command is used:

```
service eltex-ngw stop
```

To start the service after stopping:

```
service eltex-ngw start
```

To check if the service is operating at the moment, use the command:

```
service eltex-ngw status
```

The following message will be displayed, if the service is operating:

```
eltex-ngw start/running, process <pid>
```

or eltex-ngw stop/waiting will be displayed

```
eltex-ngw stop/waiting
```

## Configuration

### /etc/eltex-ngw/notification.properties

The main configuration file containing the following parameters:

- The configuration file for SMS gateway connection (for sending SMS to users)

```
sms.gate.outgoing.sms.config=smsc_gate.conf
```

- The configuration file for user identification by SMS sent by him:

```
sms.gate.incoming.sms.config=smpp_gate.conf
```

- The configuration file for user identification by incoming calls:

```
sms.gate.incoming.call.config=rtk_sbc.conf
```

- Configuring the size of an SMS pool and the waiting time:

```
#Gate pool settings
sms.gate.pool.size=50
sms.gate.pool.wait.millis=5000
```

- Configuring the size of an SMS pool and the waiting time. The configuration file for incoming call authorization

```
#Call gate configuration
call.gate.outgoing.call.config=smg_gate.conf
call.gate.pool.size=50
pool.wait.millis=5000
```

- The port listened by the service to receive requests for SMS sending:

```
#Port to listen for requests
server.port=8040
```

- Configuring MongoDB connection for keeping an SMS sending log

```
#============================
#=======database settings=====
#============================
#mongodb.uri=mongodb://192.168.1.1,192.168.1.2:27017/notification-gw
mongodb.host=localhost
mongodb.port=27017
#mongodb.user=user
#mongodb.password=password
mongodb.name=notification-gw
mongodb.fsfiles.store.period=7
```

To connect to replicaSet, the format mongo uri can be used. It is as follows:

```
mongodb://[username:password@]host1[:port1][,host2[:port2],...
[,hostN[:portN]]][/[database][?options]]
```

An example of connecting to replicaSet with authorization configured:

```
mongodb.uri=mongodb://
admin_ngw:password@192.168.42.224:27017,192.168.42.225:27017,192.168.42
.226:27017/notification-gw?replicaSet=clustest
```

- Connecting to the mail service

```
#============================
#=======email settings========
#============================
mail.smtp.submitter=example@eltex.loc
mail.smtp.password=password
mail.smtp.auth=true
mail.smtp.host=eltex.loc
mail.smtp.port=587
mail.smtp.sendpartial=true
mail.smtp.connectiontimeout=5000
mail.gate.pool.size=20
mail.pool.wait.millis=10000
```

To enable encryption of the mail service connection, specify the following option:

```
mail.smtp.starttls.enable=true
```

### /etc/default/eltex-ngw

contains parameters for application launch

```
JAVA_INIT_HEAP=16m
# Maximum size of Java heap
JAVA_MAX_HEAP=128m

LOG_LEVEL=info

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-
ngw"
```

JAVA_INIT_HEAP - amount of memory allocated to an application when starting the service

JAVA_MAX_HEAP - maximum amount of memory that an application can use

LOG_LEVEL - a logging level: error, warning, info, debug

JAVA_OPTS - additional options for java launch

### Configuration files to connect SMS gateways

To connect to different SMS gateways, a set of configuration templates was created. If you have not found a required template among suggested ones, contact the technical support to provide integration with your gateway.

- SMS center - smsc_gate.conf
- Seven Sky  - 7sky_gate.conf
- Zagruzka - zagruzka_gate.conf
- SMS gateway with SMPP support - smpp_gate.conf
- NetPing SMS GSM gateway - netping_gate.conf
- Fargo maestro 100 GSM gateway - serial_port.conf

Contact the technical support to ask whether it is possible to provide integration with other gateways.

## v1.14_Configuring incoming call authorization (EN)

**Configuration**

To configure incoming call authorization with SMG gateway, specify SMG gateway configuration file in call.gate.outgoing.call.config parameter of /etc/eltex-ngw/notification.properties configuration file. Example:

```
#Call gate configuration
call.gate.outgoing.call.config=smg_gate.conf
call.gate.pool.size=50
pool.wait.millis=5000
```

Configure SMG gateway interaction in smg_gate.conf configuration file (it is located in the same directory as notification.properties).

```
smg.host=<ip-address>
smg.port=3799
smg.secret=radiuspass

listen.port=1814
listen.secret=radiuspass1
```

smg.host = SMG gateway addresssmg.port = the port that listens to SMG

gatewaysmg.secret = RADIUS-Authorization key configured on SMG gateway

`listen.port` = the port that listens to NGW. Any relevant port can be configured; it is required to specify a new port on SMG gateway

`listen.secret` = RADIUS Accounting key

After configuration files are modified, restart eltex-ngw server

```
root@vagrant-ubuntu16-xenial-64-SWLC:~# service eltex-ngw restart
```

**Check**

To check SMG gateway connection, use radclient utility and make a CoA request containing a telephone number to which an incoming call should come in.

```
root@vagrant-ubuntu16-xenial-64-SWLC:~# echo Called-Station-Id="79964567890"  | radclient  -sx
192.168.1.10:3799 coa radiuspass
Sending CoA-Request of id 150 to 192.168.1.10 port 3799
        Called-Station-Id = "79964567890"
rad_recv: CoA-ACK packet from host 192.168.1.10 port 3799, id=150, length=33
        Calling-Station-Id = "73830012345"

           Total approved auths:  1
             Total denied auths:  0
              Total lost auths:  0
```

CoA-ACK with Calling-Station-id containing a telephone number from which a call will be made, should be received in response.

# v1.14_Configuring outgoing call authorization (RADIUS) (EN)

One of the integration options allows getting data on users' calls via **RADIUS** protocol. That implies that **eltex-ngw** service waits for **radacct-stop (Acct-Status-Type = Stop)** package containing a caller's telephone number in **Calling-Station-Id** parameter.

**Configuration:**

1.Specify the number of the gateway that is expecting a call from a client in **NUMBERS_FOR_INCOMING_CALLS** parameter of **/etc/eltex-ngw/rtk_sbc.conf**. In **RADIUS_PORT** and **RADIUS_SECRET** parameters, a listened port and **radius-secret** are specified.
**PHONE_NUMBER_PREFIX** parameter automatically adds the given prefix to accounting notifications on incoming calls from SBC. Configuration example:

```
RADIUS_PORT=8041
RADIUS_SECRET=1234

# prefix to be applied to the phone number in Calling-Station-Id attribute
PHONE_NUMBER_PREFIX=

# numbers for receiving incoming calls
# comma is a separator
NUMBERS_FOR_INCOMING_CALLS=88001230123
```

2. In **/etc/eltex-ngw/notification.properties** file, specify the parameter:

```
sms.gate.incoming.call.config=rtk_sbc.conf
```

3. After that, restart **eltex-ngw**.

**Check:**

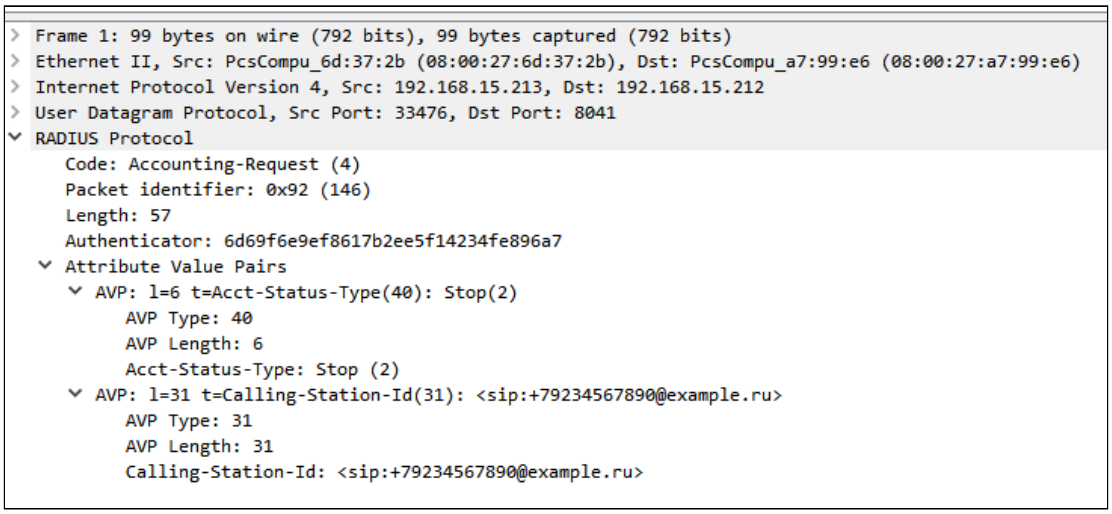
Send **acct-stop** request using **radclient** utility:

```
echo 'Acct-Status-Type = Stop, Calling-Station-Id = "<sip:
+79234567890@exmple.ru>"' | radclient localhost:8041 acct eltexsecret
```

Note that when rtk_sbc configuration is used, eltex-ngw service expects a number in the following format: <sip:telephone number@some_text> (for example, <sip:79234567890@a>). If the format is inconsistent with the one above, a processing error will occur, and the following message will be written to logs:

```
2017-10-10 00:00:00.001 [SbcRadiusReceiver] WARN  SbcRadiusReceiver:151 -
Could not extract phone from Calling-Station-Id "79234567890"
```

An example of **radacct** package that should be sent to **eltex-ngw**:




## v1.14_Sending SMS using a script

This method is used if a provider gives scripts to subscribers. When SMS messages are used for authorization, a script takes the two parameters: phone number and key (password).

### Configuration

1. To configure SMS sending using a script, specify a gateway configuration file sms_script.conf in sms.gate.outgoing.sms.config property of /etc/eltex-ngw/notification.properties file.

```
#Common gates settings
#Current gate used for each type (config name, for example smpp_gate.conf)
sms.gate.outgoing.sms.config=sms_script.conf
#For incoming sms/calls fields for numbers in configs should be set
sms.gate.incoming.sms.config=
sms.gate.incoming.call.config=
```

2. Create a script. Make it executable.
3. Specify a script path in /etc/eltex-ngw/script.conf configuration file.

```
script.path=/home/tester/test.sh
```

4. Restart **eltex-ngw** service.

```
sudo service eltex-ngw restart
```

## v1.14_Sending messages via NGW

To send text messages via NGW, a simple HTTP interface is implemented.
To send a command, curl utility is used.

To send SMS, the command should have the following format:

```
$ curl -Xpost localhost:8040/api/sms --data '{ "phone": "79831300000",
"message": "http hello"}' -H 'Content-Type: application/json' -i
```

If command processing and message sending are successful, the response will be:

```
HTTP/1.1 200 OK
Date: Wed, 13 Dec 2017 12:05:52 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
Server: Jetty(9.4.3.v20170317)

{
  "code": 0,
  "detail": "Sms is sent successfully on Smsc. ID: adc2f952-3a24-4148-910f-
d5a9b77c85c5, parts in SMS: 1, cost: 0, balance: 51.144"
}
```

If a failure occurs during command processing, for example, when the number is incorrect:

```
$ curl -Xpost localhost:8040/api/sms --data '{ "phone": "79831300000asdf",
"message": "http hello"}' -H 'Content-Type: application/json' -i
```

The server will return the following error:

```
HTTP/1.1 500 Server Error
Date: Wed, 13 Dec 2017 12:07:15 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
Server: Jetty(9.4.3.v20170317)

{"message": "Received error code = 7. Incorrect format of phone number"}
```

Command format for e-mail sending:

```
curl -Xpost localhost:8040/api/email --data '{"subject": "http email", "to":
"example@example.loc", "message": "http hello"}' -H 'Content-Type:
application/json' -i
```

The server response on a successful sending:

```
HTTP/1.1 200 OK
Date: Wed, 13 Dec 2017 12:05:27 GMT
Content-Length: 0
Server: Jetty(9.4.3.v20170317)
```

# v1.14_RADIUS (EN)


- Description
- Starting/stopping procedure
- Configuration
  - /etc/eltex-radius/local.conf
  - NAS table
  - Logging
    - Log rotation


## Description

The service is used to provide AAA mechanisms for Wi-Fi users connected with WPA-enterprise (EAP). Access points provide RADIUS authorization and authentication with the servers, and the servers request client data from a database. RADIUS also performs support functions for user authorization via ESR/BRAS.

The service is installed from the package **eltex-radius**.

## Starting/stopping procedure

To stop the service, the following command is used:

```
service eltex-radius stop
```

To start the service after stopping:

```
service eltex-radius start
```

To check the service status, use the command:

```
service eltex-radius status
```

This will be followed by a message:

```
eltex-radius start/running, process <pid>
```

if the service is running or by

```
eltex-radius stop/waiting
```

if it is not.

## Configuration

Configuration file is located in `/etc/eltex-radius`. Of all the files, the following ones can be edited:

- `local.conf` - basic parameters that may need to be edited
- `certs/server.crt` - server certificate used in EAP-TLS
- `certs/server.key` - server private key used in EAP-TLS
- `certs/ca/*.pem` - root CA certificates (it is recommended to set local.pem name for CA certificate and define it in the local.conf when configuring EAP-TLS)

Start in debugging mode: `eltex-radius -X`

### /etc/eltex-radius/local.conf

Main configuration file. Contains the following parameters:

- Listened ports configuration:

```
auth_port=1812
acct_port=1813
inner_tunnel_port=18121
```

- Configuring connection to **radius** database:

```
# MySQL database
db_host="localhost"
db_port=3306
db_login="radius"
db_password="radpass"
db_name="radius"
```

- The option than enables/disables SSID block check. If it is set to 1, users will not be able to log in on SSID blocked via EMS.

```
ssid_check_enabled=1
```

- Configuring connection to **wireless** database:

```
# MySQL 'wireless' database
wireless_db_host="localhost"
wireless_db_port=3306
wireless_db_login="javauser"
wireless_db_password="javapassword"
wireless_db_name="wireless"
```

- Connection to **PCRF**:

```
# PCRF
pcrf_host="127.0.0.1"
pcrf_port=7080
pcrf_enabled=1
```

- The name of CA certificate used for TLS authorization and server sertificate key. These parameters will be changed automatically during the running of certificate installation script included into **eltex-radius-nbi** package.

```
# EAP
ca_cert_name="local.pem"
tls_key_password="1234
```

- Configuring request proxying to another RADIUS server:

```
proxy_auth=0
proxy_domain_regex="^(.+\.)?enterprise\.root$"
proxy_host="127.0.0.1"
proxy_port=18121
proxy_secret="eltex"
```

- Enabling special authorization request processing algorithms for some vendors' devices.

```
ubi_vendor_regex="Apple|Ubiquiti"
vendor_group_enabled=1
```

- Configuring dynamic clients for authorization:

```
# Settings of runtime NAS discovery
dynamic_clients=false
dynamic_client_subnet=192.168.0.0/16
dynamic_client_lifetime=3600
dynamic_client_rate_limit=false
```

### NAS table

This table is included into **radius** database and contains addresses of clients (access points) that are allowed to send user authorization requests. If a client is not included into the table, authorization requests will be ignored. When the contents of the table is changed, restart **eltex-radius**. When EMS object tree is changed (access points are added/removed), the table is updated automatically, and **eltex-radius** is restarted.

### Logging

Server logging can be configured in a section of **/etc/eltex-radius/radiusd.conf** log file. By default, the section is as follows:

```
log {
    destination = syslog
    colourise = yes
    file = ${logdir}/radius.log
    syslog_facility = daemon
    stripped_names = no
    auth = yes
    auth_badpass = yes
    auth_goodpass = yes
    msg_denied = "You are already logged in - access denied"
}
```

Short description of significant parameters of the section is given below:

| Parameter | Description |
|---|---|
| destination | log destination that can take two values:<br>• syslog — the default, processing is done by a system Syslog daemon<br>• file — manual logging to a file specified in file parameter\| |
| file | file path that is set by default to ${logdir}/radius.loglogdir = /var/log/eltex-radius thus, a log file is located in /var/log/eltex-radius/radius.log |
| syslog_facility | facility, a log category for Syslog logging |
| auth | to log authorization requests, values yes or no are accepted |

Log rotation

For log rotation using **logrotate**, a configuration file should be created, the following is the example:

**/etc/logrotate.d/eltex-radius**

```
/var/log/eltex-radius/radius.log {
        daily
        rotate 31
        create 640 eltxrad eltxrad
        compress
        delaycompress
        notifempty
        missingok
        postrotate
                invoke-rc.d eltex-radius reload >/dev/null 2>&1 || true
        endscript
}
```

For the case considered,

- `daily` — rotate files daily;
- `rotate 31` — rotate files for the last 31 days;
- `create 640 eltxrad eltxrad` — create a new file with access rights 640, set owner to eltxrad, set group ownership to eltxrad. This is the account the server is running under;
- `postrotate` - reload the server to start logging to the created file.

## v1.14_Proxying to other RADIUS servers


- Default configuration
- Proxying authorization to another (home) RADIUS server
- Proxying authorization and accounting to home RADIUS server
- Proxying authorization and accounting to multiple RADIUS servers
- Disabling home server's status check
- Sources


| **Product Versions** | Eltex-RADIUS 1.7+ |
|---|---|

Eltex-RADIUS allows proxying to a home server. By default, the opportunity is available only for authorization requests proxying to one server. The section describes how to configure both authorization and accounting proxying to one or more servers.

### Default configuration

Proxying default configuration is located in **`/etc/eltex-radius/local.conf`** file and looks like this:

**a part of /etc/eltex-radius/local.conf file**

```
# Proxying
proxy_auth=0
proxy_domain_regex="^(.+\.)?enterprise\.root$"
proxy_host="127.0.0.1"
proxy_port=18121
proxy_secret="eltex"
```

- **`proxy_auth`** – proxying status, allowed values 0 and 1, 0 by default, disabled
- **`proxy_domain_regex`** – a regular expression that defines domains in which authorization requests will be proxiedto proxy all requests, set this parameter to **`"^(.+\.)?root$"`**
- **`proxy_host`** – an address of a home server requests will be proxied to
- **`proxy_port`** – a server's interface
- **`proxy_secret`** – a key set on a home server for Eltex-RADIUS serverremember that Eltex-RADIUS will act as NAS within such a configuration

Fine settings can be done in **`/etc/eltex-radius/proxy.conf`** in the following way:

```
proxy server {
        default_fallback = no
}

home_server auth_proxy {
        type = auth
        ipaddr = "${proxy_host}"
        port = "${proxy_port}"
        secret = "${proxy_secret}"

        response_window = 20

        #
        #  Start "zombie_period" after this many responses have
        #  timed out.
        #
#       response_timeouts = 1
        zombie_period = 40
        revive_interval = 120

        status_check = status-server
        check_interval = 30
        check_timeout = 4
        num_answers_to_alive = 3
        max_outstanding = 65536
}

home_server_pool auth_proxy_failover {
        type = fail-over
        home_server = auth_proxy
}

realm auth_proxy {
        auth_pool = auth_proxy_failover
}

realm LOCAL {
        #  If we do not specify a server pool, the realm is LOCAL, and
        #  requests are not proxied to it.
}
```

The following sections are important:

- `home_server`
- `home_server_pool`
- `realm auth_proxy`

### Proxying authorization to another (home) RADIUS server

The simplest case is proxying authorization requests to one home RADIUS server. **`/etc/eltex-radius/local.conf`** file should be modified in a following way:

**a part of /etc/eltex-radius/local.conf file**

```
# Proxying
proxy_auth=1
proxy_domain_regex="^(.+\.)?enterprise\.root$"
proxy_host="10.10.10.11"
proxy_port=1812
proxy_secret="topsecret"
```

According to the configuration, all authorization requests in enterprise.root domain hierarchy will be proxied to 1812 port of a server with 10.10.10.11 address, `topsecret` will be used as a `secret`.

⚠ According to the configuration, accounting will still be processed locally, i.e., by Eltex-RADIUS.

**`/etc/eltex-radius/proxy.conf`** file modification is not required.

### Proxying authorization and accounting to home RADIUS server

To proxy accounting requests as well as authorization requests, /etc/eltex-radius/proxy.conf file should be modified.
In the section **`home_server`**, change a value of **`type`** parameter to **`auth+acct`**:

```
home_server auth_proxy {
        type = auth+acct
        ipaddr = "${proxy_host}"
        port = "${proxy_port}"
        secret = "${proxy_secret}"

        response_window = 20

        #
        #  Start "zombie_period" after this many responses have
        #  timed out.
        #
#       response_timeouts = 1
        zombie_period = 40
        revive_interval = 120

        status_check = status-server
        check_interval = 30
        check_timeout = 4
        num_answers_to_alive = 3
        max_outstanding = 65536
}
```

In the section **`realm auth proxy`**, replace the parameter **`auth_pool`** to **`pool`**, the value should remain the same:

```
realm auth_proxy {
        pool = auth_proxy_failover
}
```

In the file **`/etc/eltex-radius/servers/default`**, add a line **`proxy_auth`** after **`preprocess`** in **`preacct`** section:

```
preacct {
        preprocess
        proxy_auth
        acct_counters64
        acct_unique
        acct_ciscoavpair

        # Parse common cisco-avp ('domain' for example)
        common_ciscoavpair
       rewrite_called_station_id

       if (${pcrf_enabled} == 0) {
           fill_ap_domain
           fill_ssid_security
       }

       files
}
```

### Proxying authorization and accounting to multiple RADIUS servers

This option requires significant modification of configuration files. Proxying to two home servers will be considered below, but the method suggested is also available for further scaling.
Edit /etc/eltex-radius/local.conf by adding host, port and secret individual parameters for each home server:

```
# Proxying
proxy_auth=1
proxy_domain_regex="^(.+\.)?root$"

proxy1_host="10.10.10.11"
proxy1_port=1812
proxy1_secret="topsecret"

proxy2_host="10.10.10.12"
proxy2_port=1812
proxy2_secret="topsecret"
```

Modify `/etc/eltex-radius/local.conf` in accordance with the configuration above. home_server section with unique name should be described for each server.
All home_server should be added to `home_server_pool` that, in turn, should be added to auth_proxy realm. As both accounting and authorization are intended to be proxied, the parameter that points to the pool should be named `pool`.

```
home_server auth_proxy1 {
        type = auth+acct
        ipaddr = "${proxy1_host}"
        port = "${proxy1_port}"
        secret = "${proxy1_secret}"

        response_window = 20

        #
        #  Start "zombie_period" after this many responses have
        #  timed out.
        #
#       response_timeouts = 1
        zombie_period = 40
        revive_interval = 120

        status_check = status-server
        check_interval = 30
        check_timeout = 4
        num_answers_to_alive = 3
        max_outstanding = 65536
}

home_server auth_proxy2 {
        type = auth+acct
        ipaddr = "${proxy2_host}"
        port = "${proxy2_port}"
        secret = "${proxy2_secret}"

        response_window = 20

        zombie_period = 40
        revive_interval = 120

        status_check = status-server
        check_interval = 30
        check_timeout = 4
        num_answers_to_alive = 3
        max_outstanding = 65536
}


home_server_pool auth_proxy_failover {
        type = fail-over
        home_server = auth_proxy1
        home_server = auth_proxy2
}

realm auth_proxy {
```

```
        pool = auth_proxy_failover
}
```

Add a line **proxy_auth** after **preprocess** to **preacct** section of **/etc/eltex-radius/servers/default** file, as described above.

> The configuration considered handles failover between home servers and is set via 'type' parameter in home_server_pool section. The load-balancing mode is also available, follow link 2 in the "Sources" section to get further information.

### Disabling home server's status check

When proxying is performed, home server's status checking mechanism is enabled. If a home server does not respond for some time, and then becomes available again, it should respond to **status-server** request — only after that, proxying will resume.

During operation, it would appear that a home server can not respond to **status-server**, or it is not appropriately configured. In such a case, the check can be disabled.

To do that, the following changes are required:

In /etc/eltex-radiu/proxy.conf file:

in home_server auth_proxy section set:

status_check = **none** , is set to status-server by default

revive_interval = **60**, 120 by default

in home_server_pool auth_proxy_failover section set:

type = **fail-over,** set to load-balance by default

After that, restart the daemon with **service eltex-radius restart**

As a result, if the connection between the servers fails, the service will become available in 60 seconds after re-establishing communication.

### Sources

1. https://wiki.freeradius.org/version4/upgrade/proxy
2. https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/raddb/proxy.conf

## v1.14_Rotation and accounting storage

- Automatic start configuration

- Configuration files
  - /etc/eltex-radius-db/manager-login
  - /etc/eltex-radius-db/three_years_radacct
    - Automatic data export to a remote storage
      - Configuring rcync data export
      - Configuring FTP data export
- Script logging
- Configuring e-mail notification
- Data selection when creating an archive


In SoftWLC v.1.8.1 and above, user accounting archiving mechanism is implemented with the help of shell scripts using cron utility. The scripts are included into eltex-radius-db (1.8-123) package.
A new script allows performing more flexible setup of data archiving, cleaning and export algorithm.
Partitioning is done weekly, not monthly, that allows keeping less data in a database.
Data archiving is done weekly.

### Automatic start configuration

When eltex-radius-db package is installed/updated, a user will be offered to add the script running to cron:

```
Do you want to add ThreeYearsRadacct monitor to cron? [Y/n] y
CRON server will be restarted with "service cron restart"
cron stop/waiting
cron start/running, process 7042
```

If a user agrees to add the script to cron, **/etc/cron.d/eltex-radius-db** file with the following contents is created:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# cat /etc/cron.d/eltex-radius-db
# Launch every Monday
0 0 * * 1 root /usr/lib/eltex-radius-db/three_years_radacct_wrap.sh
```

⚠ If a user presses n, the launch line will be commented out, and cron will not be restarted within the installation process.

⚠ If there is a need to change the time of script launch, edit cron sequence in **/etc/cron.d/eltex-radius-db** and then restart cron service.

# Creating partitions

In previous versions, raddact table partitioning was done monthly by launching a script creating partitions for a month ahead on a regular basis.
In the current version, partitions are created weekly. To create new partitions, **/etc/cron.daily/radius-db-partitions** script is used. The script is launched daily and checks for a partition for next week. If there are no partitions, a new partition is created.

When eltex-radius-db is installed for the first time, partitions for previous 3 years and for next week (regarding current server time) are created.
When upgrading from freeradius-eltex-db versions earlier than 3.2.0 with no month partitioning, a database is upgraded. This process may take a long time.
When upgrading from later versions, old partitions splitted per month will remain the same, and new partitions will be created monthly.

## Configuration files

### /etc/eltex-radius-db/manager-login

The file contains login and password for database connection.

> The script is intended to be run on the database server computer, so the address of database server is not specified by default.

### /etc/eltex-radius-db/three_years_radacct

The file contains monitor configuration.

| Parameter | Default value | Description |
|---|---|---|
| **ARCHIVE_DIR** | "/var/ems-backup/radius/csv/" | The directory for storing accounting archives. |
| **PART_WEEK** | 26 | Accounting storage time is measured in weeks. On expiry of the time, data is removed from the database. |
| **ARCHIVE_WEEK** | 156 | Archive storage time for **$ARCHIVE_DIR** directory is measured in weeks. On expiry of the time, archives are removed from the directory. |

| | | |
|---|---|---|
| **NOTIFICATION_ADDR** | | administrator's e-mail address for sending notifications on script operation errors.<br><br>⚠ To send e-mail notifications, install and configure **mailutils** and **ssmtp** packages. The instruction on configuring the packages can be found in this manual.<br><br>ⓘ In **mailutils 1:2.99.99-1ubuntu2** and higher versions, simultaneous sending to more than one recipients is supported. Recipients should be added to a space-separated list in double quotes. For example: "example@mail.org example2@mail.org" |

Automatic data export to a remote storage

In addition to archiving and accounting rotation, the script is able to perform automatic export of archived data to remote servers. The export is implemented with the help of rsync and FTP.

Configuring rcync data export

⚠ Rsync and sshpass packages should be installed on the server for the service to run

| Parameter | Default value | Description |
|---|---|---|
| **RSYNC_REMOTE** | N | Enabling rsync data export to a remote storage. |
| **RSYNC_REMOTE_HOST** | 192.168.0.1 | Remote storage address for rsync data export. |
| **RSYNC_REMOTE_PORT** | 22 | The port for rsync connection. |
| **RSYNC_REMOTE_USER** | admin | Username for rsync connection. |
| **RSYNC_REMOTE_PASSWORD** | password | User password for rsync connection. |
| **RSYNC_REMOTE_PATH** | "/var/ems-backup/radius/csv/" | The path to save archives (in a remote storage). |

Configuring FTP data export

⚠ The server should have **lftp** utility pre-installed for the service to run.

| Parameter | Default value | Description |
|---|---|---|
| **FTP_REMOTE** | N | Enabling FTP data export to a remote storage. |
| **FTP_REMOTE_HOST** | 192.168.0.1 | Remote storage address for FTP data export. |
| **FTP_REMOTE_PORT** | 21 | A port for FTP connection. |

| | | |
|---|---|---|
| **FTP_REMOTE_USER** | admin | Username for FTP connection. |
| **FTP_REMOTE_PASSWORD** | password | User password for FTP connection. |
| **FTP_REMOTE_PATH** | "/var/ems-backup/radius/csv/" | The path to save archives (in a remote storage). |

### Script logging

Script operation logs are saved to **/var/log/eltex-radius-db/** directory.
Log rotation is configured in **/etc/logrotate.d/radacct**.

### Configuring e-mail notification

**mailutils ssmtp** packages (from standard Ubuntu repositories) are used for e-mail notifying. Quickstart guide:
Install the packages by using a command:

```
apt-get install mailutils ssmtp
```

Specify the data for SMTP server connection in **/etc/ssmtp/ssmtp.conf** configuration file, for example:

```
mailhub=192.168.1.1
AuthUser=tester@example.loc
AuthPass=password
UseTLS=NO
UseSTARTTLS=YES
```

Define a sender's address in **/etc/ssmtp/revaliases** configuration file, for example:

```
root:tester@example.loc:192.168.1.1:25
```

Process restart is not required.
To check if notifications were sent, use a console command:

```
echo "This is a test message from console" | ssmtp -v -s test-
destination@example.loc
```

### Data selection when creating an archive

When archives are created, data is exported according to the following condition:

```
(starttime <= end and starttime >= start) or (stoptime <= end and stoptime >=
start)
```

where
**start** - data selection start time;
**end** - data selection end time;
**starttime** - the time of radacct-start package receipt (user's session start time);
**stoptime** - the time of radacct-stop package receipt (user's session stop time).

The selection rule allows keeping data on sessions that have not finished by the moment of archive creation (that have not a stoptime mark). Such sessions will be finished later, and complete information on them will be added to the relevant archives.

## v1.14_DHCP server (EN)


- Description
  - Starting/stopping procedure
- DHCP server configuration
  - Network settings
    - Network Interfaces
    - Routing
  - ISC-DHCP-SERVER configuration
    - /etc/default/isc-dhcp-server
    - /etc/dhcp/dhcpd.conf
      - Configuration example
      - Configuring access points' static addresses
      - Option 82 usage
      - Option 43 usage
    - dhcpd configuration file check
  - DHCP-failover configuration
  - OMAPI configuration


### Description

It is suggested to use **ISC-DHCP-SERVER** free solution as a DHCP server. The solution allows performing the following tasks in relation to Eltex.SoftWLC project:

- Assigning primary (external) IP addresses to access points with option 43 (suboptions 11 and 12) that makes it possible to create GRE tunnels to ESR.
- Assigning secondary (management, tunnel) IP addresses to access points with option 43 (suboptions 10 and 13) for AP management, detection and automatic initialization.

- Assigning IP addresses to Wi-Fi users connecting to access points.
- DHCP clients classification using option 82, option 60 and giAddrField.

### Starting/stopping procedure

To stop the service, the following command is used:

```
service isc-dhcp-server stop
```

To start the service after stopping:

```
service isc-dhcp-server start
```

To check the service status, use the command:

```
service isc-dhcp-server status
```

This will be followed by a message:

```
* isc-dhcp-server is running
```

if the service is running, or by

```
* isc-dhcp-server is not running
```

if it is not.

## DHCP server configuration

> The solutions provided are relevant to typical network organization schemes, but they may differ from the configuration required for your network!

## Network settings

### Network Interfaces

DHCP server should have interfaces in three subnets:

- ***inner operator subnet*** — a subnet used for connection to operator's internal network. Administrators and operators connect to GUI EMS, and communication with SMS gateway and operator's services via NorthboundInterface is provided within the network. This subnet has a virtual interface (keepalived facility is used);
- ***outer operator subnet*** — a subnet used for connection to access points and other network devices. It has strict security policies. This subnet has a virtual interface (keepalived facility is used);
- ***outer subnet for receiving DHCP requests*** from Relay agents on operator's end equipment.

```
auto eth1.102 # Interface in outer operator's exchange network
iface eth1.102 inet static
address 192.168.114.8
netmask 255.255.255.192
network 192.168.114.0
vlan_raw_device eth1
auto eth1.100 # Interface in inner operator network
iface eth1.100 inet static
address 172.17.209.9
netmask 255.255.255.192
network 172.17.209.0
vlan_raw_device eth1
auto eth1.101 # Interface for assigning IP addresses to access points
iface eth1.101 inet static
address 10.203.5.7
netmask 255.255.255.192
network 10.203.5.0
vlan_raw_device eth1
```

### Routing

DHCP server should have access to three subnets:

**10.203.32.0** — for assigning primary IP addresses to access points;
**192.168.200.0** — for assigning management IP addresses to access points;
**100.65.64.0** — for assigning IP addresses to client devices.

Example of route configuration in **/etc/network/interfaces** file.

```
up ip route add 100.65.64.0/22 via 192.168.114.10
up ip route add 192.168.200.0/22 via 192.168.114.10
up ip route add 10.203.32.0/19 via 10.203.5.1
```

### ISC-DHCP-SERVER configuration

/etc/default/isc-dhcp-server

The file contains basic settings, in particular the list of network interfaces used:

```
INTERFACES="eth1.101 eth1.102"
```

/etc/dhcp/dhcpd.conf

DHCP server's address pool configuration.

Configuration example

```
default-lease-time 60;
max-lease-time 120;
log-facility local7;
class "ELTEX-DEVICES" {
match if (
(substring (option vendor-class-identifier, 0, 14) = "ELTEX_WEP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTEX_WOP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTX_WEP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTX_WOP-12AC")
);
}
subnet 192.168.114.64 netmask 255.255.255.192 {}
subnet 10.203.5.64 netmask 255.255.255.192 {}
#first IP-subnet for assigning primary addresses to access points
subnet 10.203.32.0 netmask 255.255.254.0 {
pool {
option routers 10.203.32.2;
range 10.203.32.130 10.203.32.230;
failover peer "dhcp-failover";
option vendor-encapsulated-options 0B:0c:31:30:2E:32:30:33:2E:35:2E:
31:31:32:0C:0C:31:30:2E:32:30:33:2E:35:2E:31:31:33;
allow members of "ELTEX-DEVICES";
}
}
#managed IP-subnet for assigning secondary addresses to access points
subnet 192.168.200.0 netmask 255.255.252.0 {
pool {
option routers 192.168.200.5;
range 192.168.200.120 192.168.200.164;
failover peer "dhcp-failover";
option vendor-encapsulated-options A:F:31:39:32:2E:31:36:38:2E:31:31:34:2E:
31:30:34;
allow members of "ELTEX-DEVICES";
}
}
#User IP-subnet for users (clients)
subnet 200.65.64.0 netmask 255.255.240.0 {
pool {
option routers 200.65.64.5;
range 200.65.64.200 200.65.64.250;
failover peer "dhcp-failover";
option domain-name-servers 172.16.0.1, 8.8.8.8;
}
}
```

Configuring access points' static addresses

If predetermined IP addresses of access points (secondary addresses) should be used in management network, a list of static hosts can be configured. Take the following steps in order to avoid **/etc/dhcp/dhcpd.conf** overload:

1. Create a file that includes the list and may be located in any directory, for example **/var/lib/dhcp/ touch /var/lib/dhcp/hosts.**

2. Add entries to the file.

**Entry format**

```
host wep_01 { hardware ethernet a8:f9:4b:b0:00:00; fixed-address
192.168.1.1; }
```

Where
**host wep_01** — hostname.
**hardware ethernet a8:f9:4b:b0:00:01** — MAC address of a device. Note that in order to get a secondary address, an access point uses MAC one greater than the MAC used for primary address getting.
**fixed-address 192.168.200.133** — IP address of a device.

3. Add the following line to AP address pool:

```
include "/var/lib/dhcp/hosts";
```

4. For DHCP server to be able to read the file, set the owner using the command:

```
chown dhcpd:dhcpd /var/lib/dhcp/static/hosts
```

5. Allow reading the file in AppArmor by adding the following line to **/etc/apparmor.d/usr.sbin.dhcpd** file (the line should end with a comma):

```
/var/lib/dhcp/hosts r
```

6. Restart services

```
service apparmor restart
service isc-dhcp-server restart
```

Pool configuration example:

```
subnet 192.168.200.0 netmask 255.255.252.0 {
pool {
option routers 192.168.200.5;
range 192.168.200.120 192.168.200.164;
option vendor-encapsulated-options A:F:31:39:32:2E:31:36:38:2E:31:31:34:2E:
31:30:34;
include "/var/lib/dhcp/hosts";
}
}
```

The lists should be created on both servers and kept updated. Restart servers after changing the lists' contents.

Option 82 usage

If option 82 is required, new classes should be created as follows:

```
class "NEW_class" {
match if (
(option agent.circuit-id = "E320-1-210:GigabitEthernet
1/0/2.25030007:2503-7")
and
(
(substring (option vendor-class-identifier, 0, 14) = "ELTEX_WEP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTEX_WOP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTX_WEP-12AC") or
(substring (option vendor-class-identifier, 0, 14) = "ELTX_WOP-12AC")
)
);
}
```

*The created class should be defined in a pool,* for example:

```
subnet 192.168.200.0 netmask 255.255.252.0 {
pool {
option routers 192.168.200.5;
range 192.168.200.120 192.168.200.164;
option vendor-encapsulated-options A:F:31:39:32:2E:31:36:38:2E:31:31:34:2E:
31:30:34;
allow members of "NEW_class";
}
}
```

After that, addresses from the pool will be assigned only to devices of this class.

Option 43 usage

The option is used to transfer vendor-specific data to DHCP clients.
The following suboptions are used in SoftWLC:

| Suboption | Description |
|---|---|
| **10** | EMS server address. |
| **11** | the address for management tunnel creation. |
| **12** | the address for data tunnel creation |
| **13** | the option for identifying carrier network area the access point belongs to |

According to RFC2132, the format is as follows:

```
When encapsulated vendor-specific extensions are used, the
information bytes 1-n have the following format:

 Code   Len   Data item        Code   Len   Data item       Code
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|  T1 |  n  |  d1 |  d2 | ... |  T2 |  n  |  D1 |  D2 | ... | ... |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

The option is transmitted in HEX format (hexadecimal notation). **All data should be converted from ASCII to HEX.**
All the values are separated by a colon ':', and the line ends with a semicolon ';'.
Option examples:

- In the primary address pool, option 43 (suboptions 11 and 12) is specified as follows:

```
option vendor-encapsulated-options 0B:0B:31:30:2E:32:30:33:2E:35:2E:31:30:0C:
0B:31:30:2E:32:30:33:2E:35:2E:31:31;
```

Decoding:
suboption 11, 11 symbols long, contains the address 10.203.5.10;
suboption 12, 11 symbols long, contains the address 10.203.5.11;

- In the secondary address pool, option 43 (suboption 10) is specified as follows:

```
option vendor-encapsulated-options 0A:0D:31:39:32:2E:31:36:38:2E:31:31:34:2E:
34;
```

Decoding:
suboption 10, 13 symbols long, contains the address 192.168.114.4;

- Suboption 13 is specified as follows:

```
option vendor-encapsulated-options 0D:0A:65:6c:74:65:78:2e:72:6f:6f:74;
```

Decoding:
suboption 13, 10 symbols long, contains the domain: eltex.root

⚠ If several suboptions should be transferred in a pool, they should be written in the same line. E.g. for suboptions 10 and 13, it will look like this:

```
option vendor-encapsulated-options 0A:0D:31:39:32:2E:31:36:38:2E:
31:31:34:2E:34:0D:0A:65:6c:74:65:78:2e:72:6f:6f:74;
```

dhcpd configuration file check

To check a configuration file for syntax errors without restarting DHCP server and applying a configuration, use dhcpd utility.
To run a check, launch dhcpd utility with -t modifier. If the configuration file is not located in the default directory, add -cf modifier

```
dhcpd -t -cf /path/to/dhcpd.conf
```

example:

```
root@vagrant-ubuntu-trusty-64-test1111:~# dhcpd -t -cf /etc/dhcp/
dhcpd_test.conf
Internet Systems Consortium DHCP Server 4.2.4
Copyright 2004-2012 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
/etc/dhcp/dhcpd_test.conf line 97: semicolon expected.
range
^
/etc/dhcp/dhcpd_test.conf line 105: Pool declaration with no address range.
}
^
Pool declarations must always contain at least
one range statement.
Configuration file errors encountered – exiting
```

### DHCP-failover configuration

Add a definition to **/etc/dhcp/dhcpd.conf** configuration file
On the first server:

```
failover peer "dhcp-failover" {
primary;
address 192.168.114.8;
port 647;
peer address 192.168.114.9;
peer port 647;
max-response-delay 30;
max-unacked-updates 10;
load balance max seconds 3;
auto-partner-down 180;
mclt 1800;
split 128;
}
```

On the second server:

```
failover peer "dhcp-failover" {
secondary;
address 192.168.114.9;
port 647;
peer address 192.168.114.8;
peer port 647;
max-response-delay 30;
max-unacked-updates 10;
load balance max seconds 3;
auto-partner-down 60;
}
```

Add the following line to reserved pools (192.168.200.0 subnet)

```
failover peer "dhcp-failover";
```

Server time synchronization is essential for DHCP-failover operation. If desynchronization occurs, failures are possible.

### OMAPI configuration

To set monitoring and DHCP servers' status check, generate a key and specify it in DHCP server configuration file. At first, generate keys by adding -K modifier and by specifying destination directory

```
root@vagrant-ubuntu-trusty-64-test1111:~# dnssec-keygen -K /etc/dhcp/ -r /dev/urandom -a HMAC-MD5
-b 512 -n HOST omapi_key
Komapi_key.+157+35749
```

Get the key

```
root@vagrant-ubuntu-trusty-64-test1111:~# cat /etc/dhcp/Komapi_key.+157+35749.key | awk '{print
$7 $8}'
kvxcUNEtu0137tWK/uEKU/MSQxinN0lTifbLwaQd0SvvhtW+PpvlHqSbHJnNLIfo7KSA7KFWtjoEUqIIJXgxmg==
```

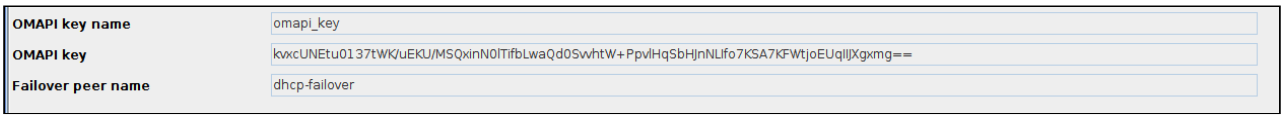
Specify the obtained key, encryption algorithm, interface and omapi_key name in DHCP server configuration file

```
key omapi_key {
        algorithm HMAC-MD5;
        secret "kvxcUNEtu0137tWK/uEKU/
MSQxinN0lTifbLwaQd0SvvhtW+PpvlHqSbHJnNLIfo7KSA7KFWtjoEUqIIJXgxmg==";
             };

omapi-port 7911;
omapi-key omapi_key;
```

Restart isc-dhcp-server

```
service isc-dhcp-server  restart
```

The only thing left to do is to specify EMS OMAPI key name, OMAPI key and Failover peer name in access settings




## v1.14_dhcp.leases files rotation

When isc-dhcp-server and AppArmor module are working together, leases file rotation problem often occurs, because there are no file privileges. It is a common problem, more information can be found here: https://bugs.launchpad.net/ubuntu/+source/isc-dhcp/+bug/1186662. The dhcp.leases file rotation problem may lead to DHCP server unstable operation.

### dhcp.leases file rotation problems diagnostics

#### DHCP server's logs analysis

When restarting isc-dhcp-server, the following entries can be found in logs.

```
Feb 27 05:43:17 gateway dhcpd: Can't create new lease file: Permission denied
```

When leases file size is exceeded by several gigabytes, the following errors may occur during DHCP server restart

```
/var/lib/dhcp/dhcpd.leases: file is too long to buffer.
```

Checking lease files creation date

Run the command:

```
$ ls -l /var/lib/dhcp/
-rw-r--r-- 1 root    root    41634468 Nov. 27 08:53 dhcpd.leases
-rw-r--r-- 1 root    root    40987441 Nov. 27 08:11 dhcpd.leases~
```

dhcpd.leases~ creation date should not differ from dhcpd.leases file by more than 1 hour. Rerun ls -l /var/lib/dhcp/ command and make sure the size of dhcpd.leases increases. If the conditions are met, dhcpd.leases file rotation works normally.

If the time difference is more than 1 hour, and dhcpd.leases file is significantly larger than dhcpd.leases~, rotation does not work.

Rotation failure example:

```
$ ls -l /var/lib/dhcp/
total 114776
-rw-r--r-- 1 root root   9644913 Nov 27 06:02 dhcpd.leases~
-rw-r--r-- 1 root root 107878109 Nov 27 09:56 dhcpd.leases
```

## Configuring file rotation on the server

To configure dhcpd.leases rotation, change dhcpd user to root in DHCP server configuration file (only those lines that need changes are given below):

```
if ! dhcpd -user root -group root -t -q -4 -cf $CONFIG_FILE > /dev/null 2>&1; then
dhcpd -user root -group root -t -4 -cf $CONFIG_FILE
chown root:root /var/run/dhcp-server
chown root:root /var/lib/dhcp /var/lib/dhcp/dhcpd.leases
chown root:root /var/lib/dhcp/dhcpd.leases~
exec dhcpd -user root -group root -f -q -4 -pf /run/dhcp-server/dhcpd.pid -cf $CONFIG_FILE
$INTERFACES
```

Change /run/dhcp-server/dhcpd.pid owner from dhcp to root:

```
chown root:root /run/dhcp-server/dhcpd.pid
```

When configuration is changed, restart DHCP server using the command:

```
sudo service isc-dhcp-server restart
```

After that, check if DHCP server operates correctly:

```
$ tail -f /var/log/dhcp.log
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: All rights reserved.
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: For info, please visit
https://www.isc.org/software/dhcp/
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: Internet Systems Consortium
DHCP Server 4.2.4
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: Copyright 2004-2012 Internet
Systems Consortium.
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: All rights reserved.
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: For info, please visit
https://www.isc.org/software/dhcp/
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: Wrote 0 class decls to
leases file.
 Nov 27 13:01:49 vagrant-ubuntu-trusty-64 dhcpd: Wrote 3210 leases to leases
file.
 Nov 27 13:01:50 vagrant-ubuntu-trusty-64 dhcpd: DHCPREQUEST for 172.30.3.252
from e0:d9:e3:50:71:e1 (WEP-2ac) via eth2
 Nov 27 13:01:50 vagrant-ubuntu-trusty-64 dhcpd: DHCPACK on 172.30.3.252 to
e0:d9:e3:50:71:e1 (WEP-2ac) via eth2
 Nov 27 13:02:04 vagrant-ubuntu-trusty-64 dhcpd: DHCPREQUEST for 172.30.3.235
from a8:f9:4b:aa:36:59 via eth2
 Nov 27 13:02:04 vagrant-ubuntu-trusty-64 dhcpd: DHCPACK on 172.30.3.235 to
a8:f9:4b:aa:36:59 via eth
```

## v1.14_Admin Panel (EN)


- General information
- Entering the system
- Interface description
    - Navigation
    - Using filters
        - Selecting a domain
    - Export of information
    - Restricting control elements visibility
    - Managing expanded statistics modal dialogs
    - Working with tables
        - Configuring table content
        - Table navigation
        - Selecting entries
- Admin Panel menu

- Start page
  - Notifications
- Statistic of a provider
  - Quotas
  - Summary data
  - Graphic
  - Session statistic Profile
  - SSID Groups
  - AP groups
  - Access points
  - Confirmation methods
- SMS Statistic
  - SMS statistic by time
  - SMS statistic by group
  - Outgoing SMS
- Hotspot/Enterprise statistics
  - Control elements
  - Users
  - Service
  - Traffic (Hotspot/Enterprise)
  - Re-visits
  - User sessions (Hotspot/Enterprise)
    - Standard control elements:
    - Searching for user sessions
    - Grouping mode
    - Sampling dates range
    - Merging sessions
- Services and tariffs
  - Tariffs
    - Tariffs for access points
      - Enterprise tariffs
      - Tariffs for portal authorization using Eltex access points
    - PCRF/BRAS
  - PCRF services
  - PCRF scenarios
- Wi-Fi users
  - Enterprise
    - Entries filtering
    - Adding and editing an entry
    - Viewing statistics and getting a TLS certificate
    - Viewing and changing quotas
    - Deleting entries
  - Hotspot users
    - Guest self-registration on the portal
    - User accounts prior creation
    - Hotspot users' traffic and time quotas
    - Time and traffic quota for Hotspot BRAS users
  - Vouchers

        - Adding a pool of entries
        - Enabling vouchers
        - Deleting a pool
    - Blocking Account
        - Filtering lists
        - Adding a list
        - Viewing and editing a list
        - Deleting a list
    - Block by def
        - Creating a list
    - Top active users Enterprise
        - Blocking operations
        - Group actions for blocking
    - Top active users Hotspot
- Access points
    - Devices
    - Problem devices
    - Offices status
    - Map
- Event log
    - Event log
    - Wi-Fi users event log
- Wireless networks
    - Editing wireless networks
        - Editing networks with portal authorization
        - Editing networks with WPA-personal authorization
        - Editing networks with WPA-enterprise authorization
    - Creating tasks for automatic password changing
        - Creating a task for password changing in networks with WPA-enterprise authorization
        - Creating a task for password changing in networks with WPA-personal authorization
        - Configuring a schedule
- Scheduler
- Advertising platform
- Settings
- PCRF settings
    - L2 subnets
    - PCRF info
    - CoA log
    - MAC bonds
    - URL lists
- Reference
    - Contact technical support
    - Feedback/claims
    - About
    - License
- Law information

## General information

Wi-Fi B2B Admin Panel is a part of the Wi-Fi Platform (SoftWLC). According to the provider's level scenario, the Wi-Fi B2B Admin Panel allows delegating the service setting to provider's clients (legal entities), And in particular obtaining statistical information on a service provided and everything about W-Fi users' accounts. The program is based on a client-server technology and allows performing remote access using a browser and classic unique login-password pairs.

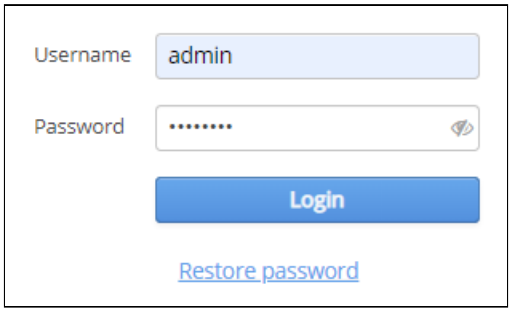
## Entering the system

To enter the interface of Wi-Fi B2B Admin Panel, open your browser and specify a server address and a service name in an address bar according to the following form: http://<server's IP address>:8080/wifi-cab/

For authentication in the program, fill in corresponding fields with a login and a password. Then click " **Login** " or press <Enter>.

After installing a new system, it is possible to access it under the login "**admin**" with a password "**password**".

⚠ It is highly recommended to change an admin password when configuring the system!




After entering the Admin Panel, the tab *"Start page"* is opened by default. To log out from the system, the button *"Logout"* located in the bottom part of the navigation bar is used.

## Interface description

### Navigation

Navigation is implemented with the help of a bar located in the left part of the screen. The navigation bar helps to choose a configuration/monitoring section. A subsection (tab) is selected in the horizontal

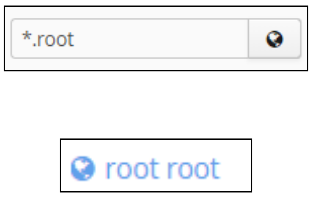
navigation element called *"Tabs"* and located in the upper part of the screen. Tabs set depends on a parent section. In the right and the main part of the interface elements for viewing and editing objects of a current tab are located.

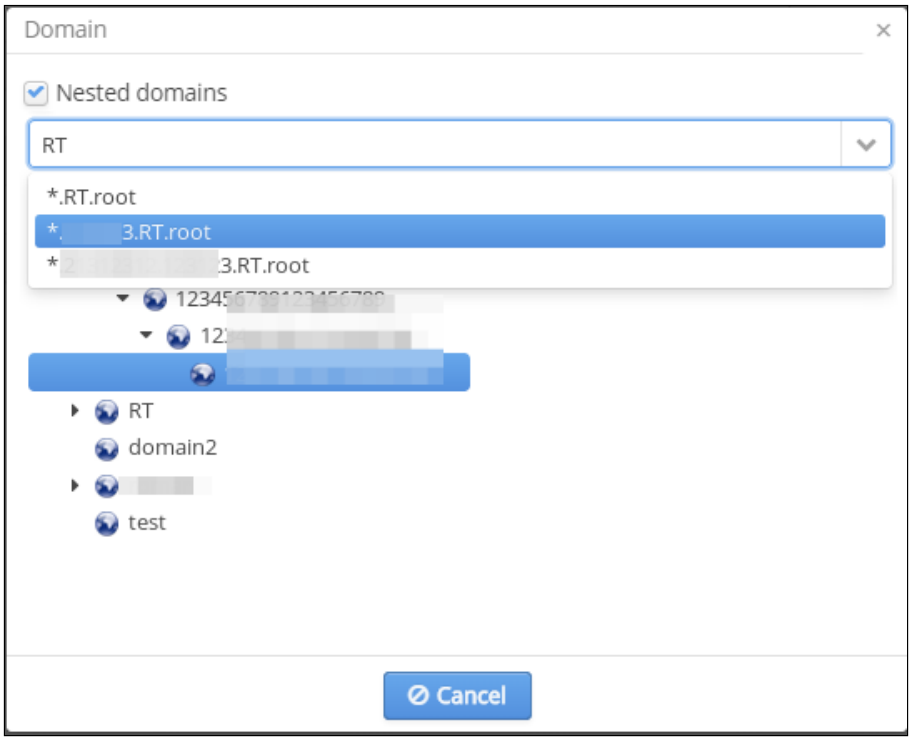
### Using filters

In some tabs, displayed data can be filtered. Despite differences between filter parameters and displayed data, the same principle of interaction with the interface is applied to all cases. When a page with no filters set is accessed, the program displays information for the last day (this period can be changed in settings). It is done to reduce the load on a database server.

Click the button " **Reload** " after any change of filter parameters. To reset all fields of a filter, use the button " **Clear** ". After this operation, a page is updated automatically.

### Selecting a domain



To select a domain on which data filtering for displaying statistics in the form of different tables and diagrams is implemented, a special widget is used.

In the widget window, the checkbox "Nested domains" that allows performing search and filtering within a certain domain and its subdomains can be found.

A field for text search of domains is located below. When symbols are entered to this field, a search is started immediately. All domains containing a symbol sequence specified in the field will be offered to a user in a drop-down menu. When one of the suggested domains is clicked with the left mouse button, its value will be saved to a filter, and the window will be closed.

A domain tree that helps to find a required domain in the structure is located under the search field. When a domain is clicked with the left mouse button, its value will be saved to a filter, and the window will be closed.

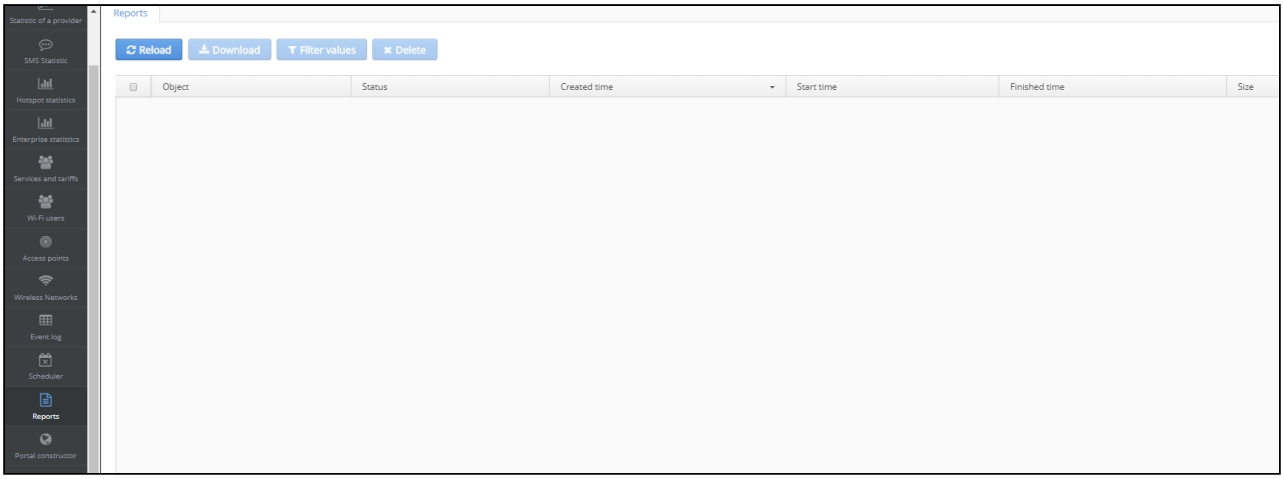
Click the button "Cancel" to save a previously selected value and close a window.

Click the button "Clear" to delete a previously selected value and close a window.

## Export of information

The Admin Panel interface provides an opportunity to export data displayed on the screen to a PDF file and to save it to a local computer of a system operator (administrator). To start writing a report file, click the button "**Export** ".

When file writing is started, a new task is created. Its status can be seen in the lower right corner of the screen. When a report is generated, it can be downloaded. Generated reports and information on them can be viewed in the corresponding section.




Reports are downloaded as .csv files (this format can be opened with Microsoft Excel).

All exported text files are downloaded in UTF-8 encoding. This should be taken into consideration when viewing files under Windows or Mac. I.e., encoding should be specified explicitly when opening a file with Microsoft Excel or other Microsoft Office programs. When Linux operating system is used, the basic packages OpenOffice.org and LibreOffice automatically open files with text in UTF-8 encoding.

### Restricting control elements visibility

Wi-Fi B2B Admin Panel is a multi-user system. That implies that different users have different rights (privileges) and different visibility area. Detailed description is given in the sections "**System roles**" and "**System users**" in the section "Admin Panel administration". Availability of certain sections and tabs depends on a user's rights. A user can also be permitted to perform only read operations or read and write operations.

If a user can perform only read operations, all control elements that allow data changing (for example, the following buttons: **"Add ",** " **Delete"** and others) will be switched to the inactive mode.

### Managing expanded statistics modal dialogs

In some sections, expanded statistics and other information are put into modal dialogs displayed over the program main interface. The main control elements of such dialogs are described below:

- Click the icon "+" to spread a window to full screen;
- Click "-" to return a window size to initial state;
- Click "x" in the right upper corner to close a window.

### Working with tables

In the program interface, some information is displayed in tabular form. Some tables are intended to display information (e.g., statistics), other tables allow data management (e.g., Wi-Fi users lists). Depending on a table type, functional features for table management are different for different tabs.

#### Configuring table content

Click the button  in the right upper corner of the table to edit its content. The functionality gives an opportunity to specify which columns should be displayed.

#### Table navigation

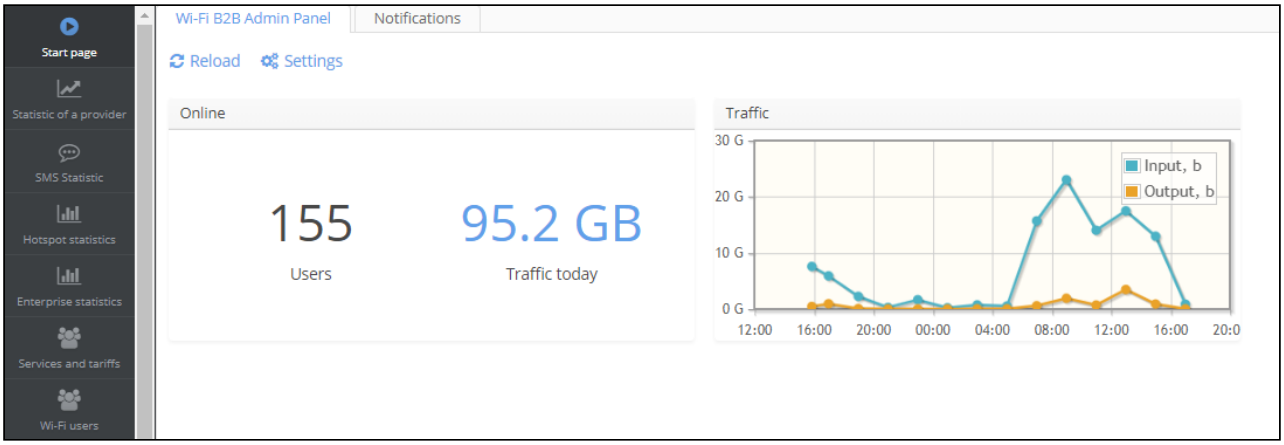
The number of entries displayed on a page simultaneously is specified in the field" **Items per page** ", a page number is specified in the field **"*Page*"** . To navigate between pages, the arrows on the right and on the left from the field *"Page"* are used. A single arrow is for moving to the next/previous page, a double one is to display the first/the last page.

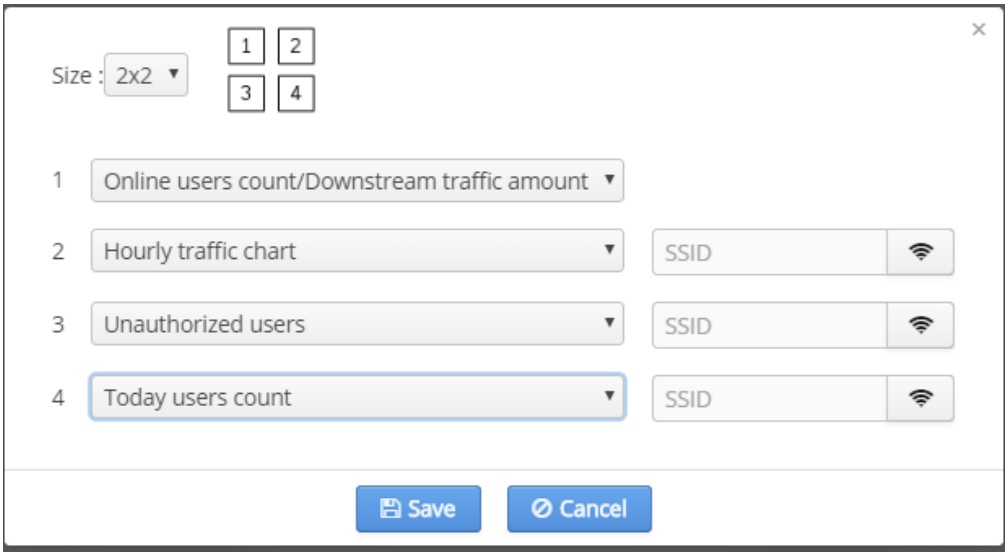
### Selecting entries

Entries for editing are selected by checking a corresponding checkbox in the first column of the table. If a checkbox in the table header is checked, all entries displayed on the screen will be selected.

## Admin Panel menu

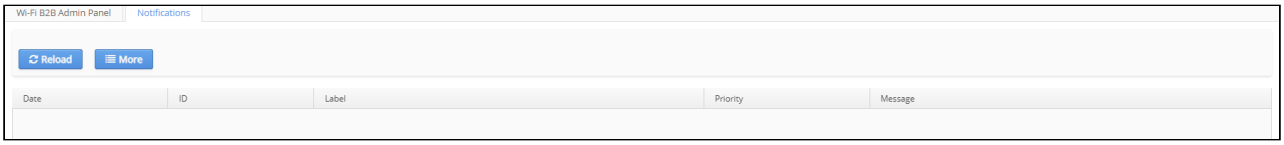
### Start page




The section contains product operation statistics. Statistics type can be customized by a user, as a contents of the page can be changed. To select diagrams that will be displayed on the Start page and specify diagram types, click the button "**Settings**".

### Notifications




The tab contains the list of critical notifications on system events. The tab is displayed only for accounts with super user rights.

To obtain more detailed information, select an entry and click "More".

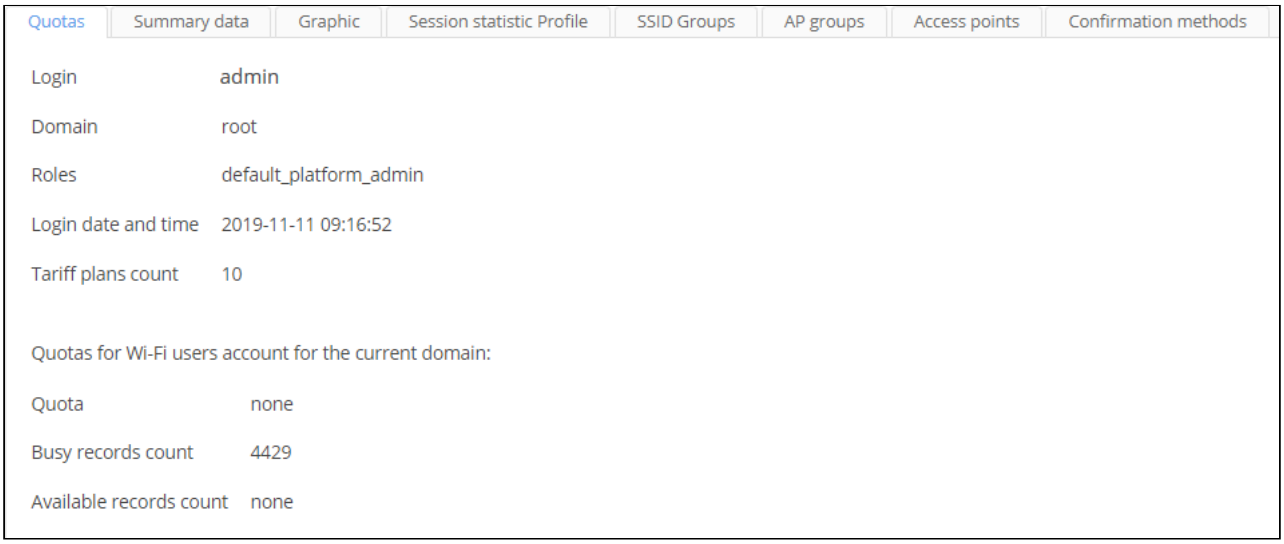
An example of a notification on modules failures.

## Statistic of a provider

The section contains statistics on the whole Platform.

> The section is available for accounts with the role of Super Administrator or Provider Staff member.

### Quotas

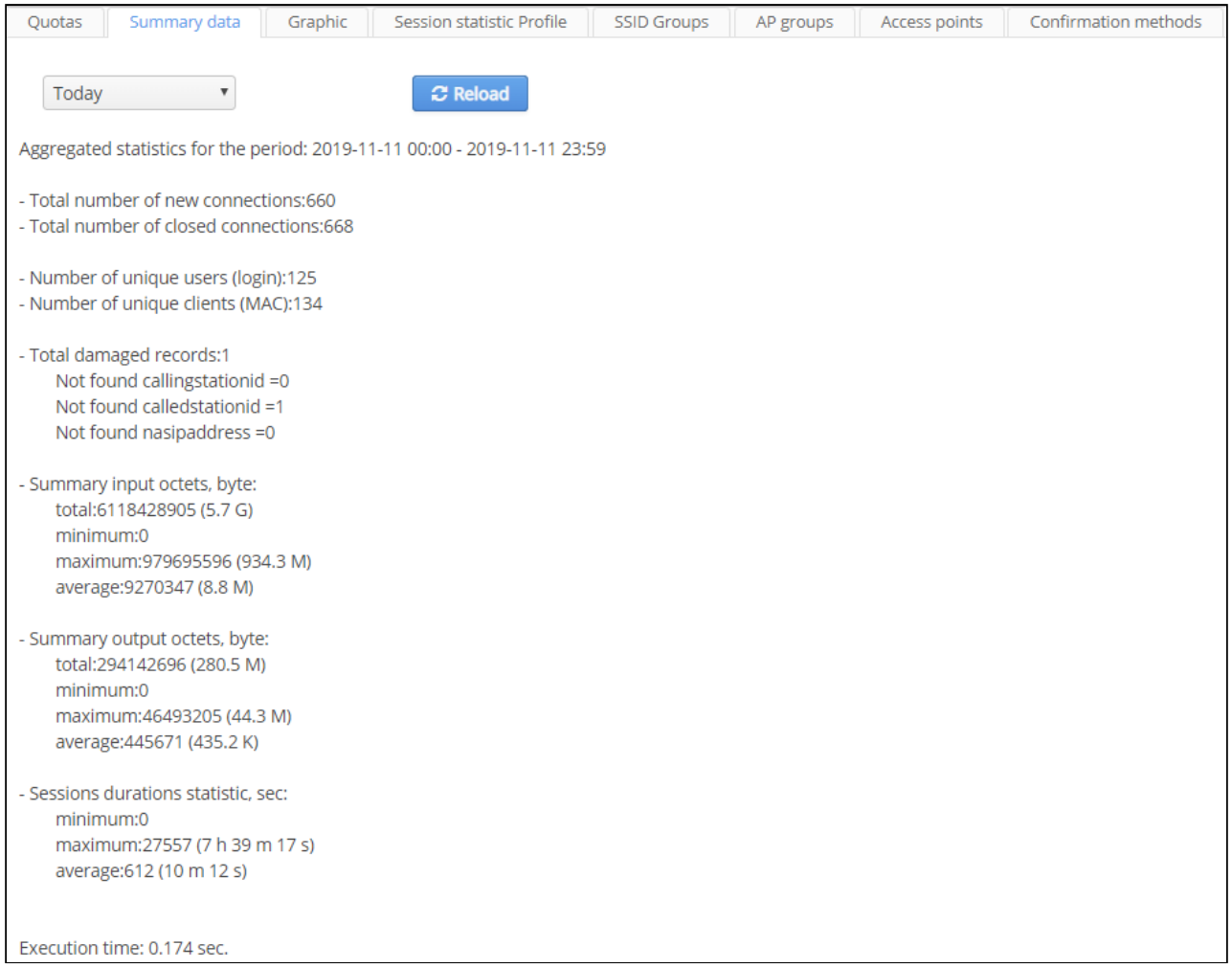



The tab contains information on a current user's account:

- Login
- Domain
- Roles
- Login date and time
- Tariff plans count

- Quotas for Wi-Fi users accounts
- Busy records count
- Available records count

Summary data

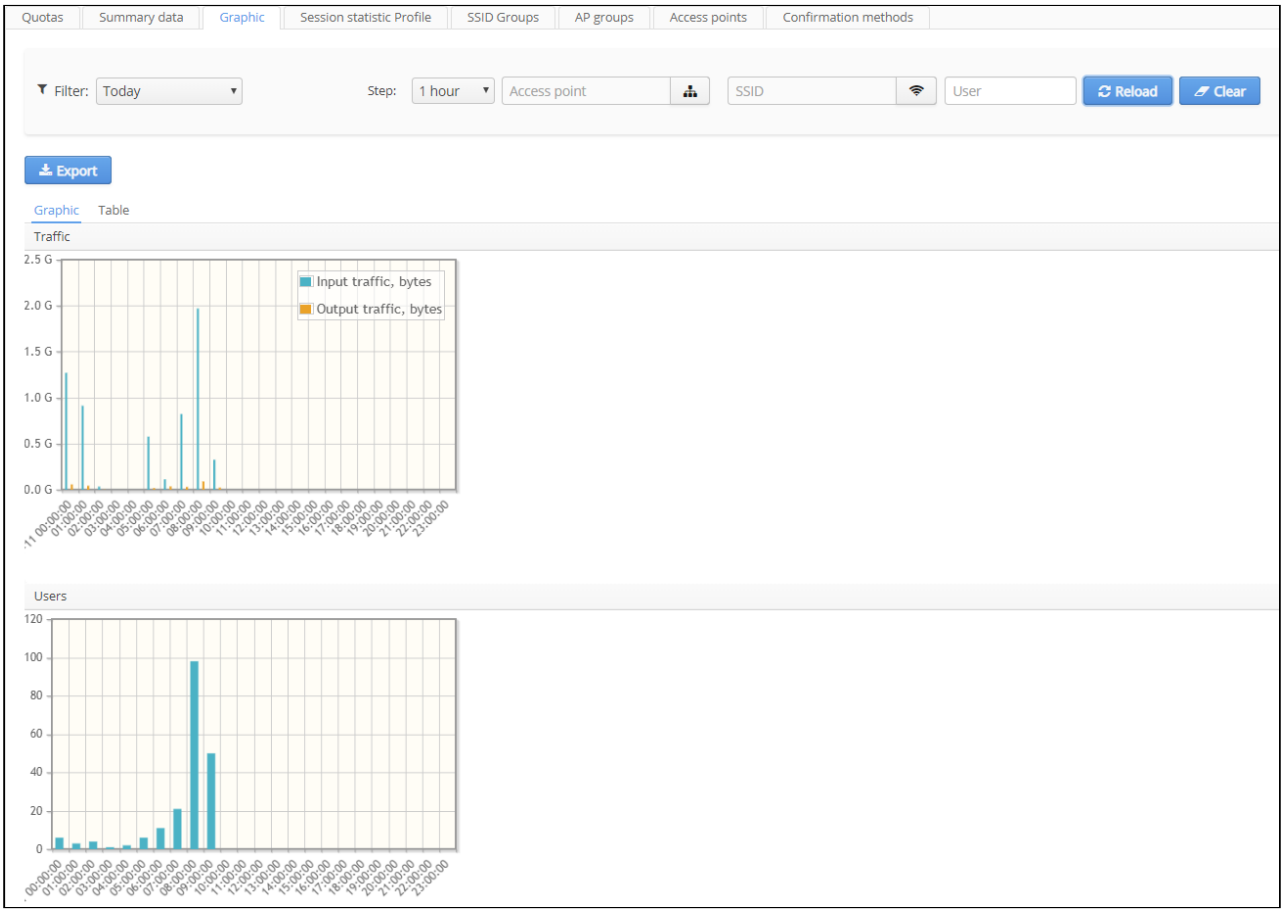



The tab contains a summary report on the "Wi-Fi Platform" operation in terms of providing end users with Wi-Fi service. Accounting (billing) information from the RADIUS service is taken into consideration. The report is generated considering a user's domain. Thus, the report will contain information on all domain and subdomain users (i.e. the main division and subsidiaries, if any) of a client's organization. The basic parameters of a summary report:

- Total number of new connections;
- Total number of closed connections;
- Number of unique users (login);
- Number of unique clients (MAC);
- total and average input octets (for Wi-Fi users);

- total and average output octets (for Wi-Fi users);
- Execution time — data on duration of sessions.

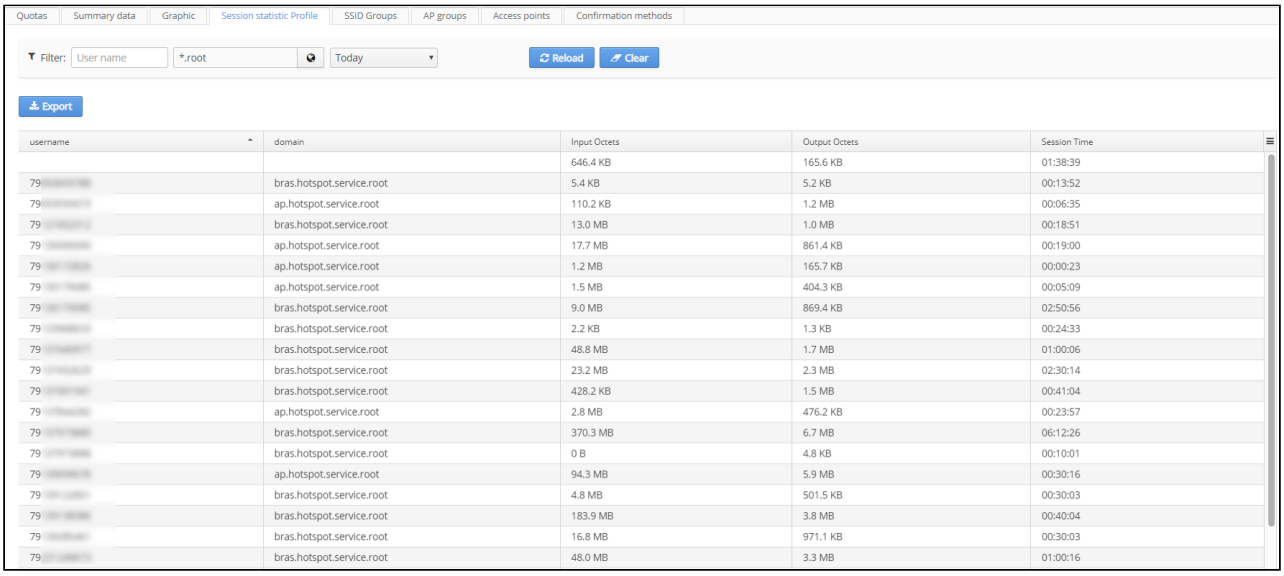
## Graphic




On this tab, different statistics on Wi-Fi Platform operation is displayed in graphic form for different time frames. Information can also be displayed in a tabular form.
When a diagram is generated, the system automatically counts the number of sections and does not allow performing requests with certain accuracy exceeded. For example, it is impossible to perform a request with hourly statistics for a month period.Diagrams contain the following information:

- *Session time* – average session time;
- *Traffic* – the volume of incoming and outgoing traffic;
- *Connections*– the number of connections;
- *Users* – the number of unique users (login);
- *Devices* – the number of unique devices (MAC addresses).

## Session statistic Profile

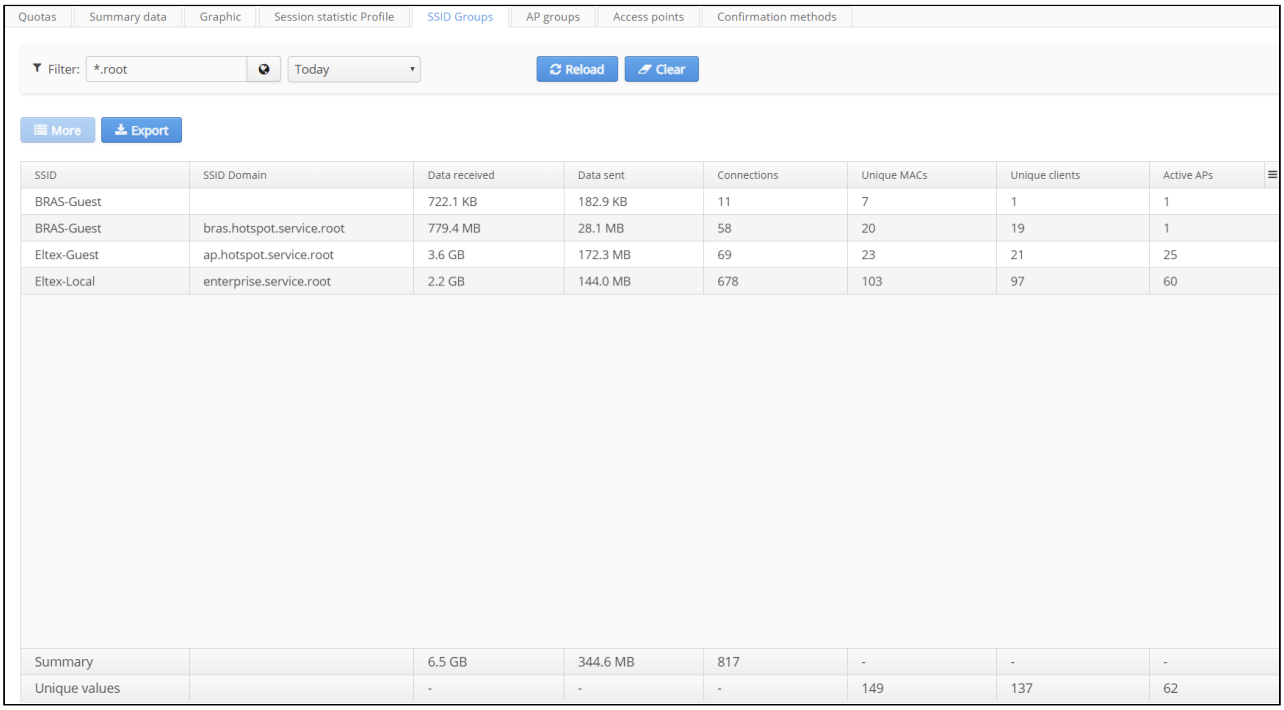



| username | domain | Input Octets | Output Octets | Session Time |
|---|---|---|---|---|
| | | 646.4 KB | 165.6 KB | 01:38:39 |
| 79 | bras.hotspot.service.root | 5.4 KB | 5.2 KB | 00:13:52 |
| 79 | ap.hotspot.service.root | 110.2 KB | 1.2 MB | 00:06:35 |
| 79 | bras.hotspot.service.root | 13.0 MB | 1.0 MB | 00:18:51 |
| 79 | ap.hotspot.service.root | 17.7 MB | 861.4 KB | 00:19:00 |
| 79 | ap.hotspot.service.root | 1.2 MB | 165.7 KB | 00:00:23 |
| 79 | ap.hotspot.service.root | 1.5 MB | 404.3 KB | 00:05:09 |
| 79 | bras.hotspot.service.root | 9.0 MB | 869.4 KB | 02:50:56 |
| 79 | bras.hotspot.service.root | 2.2 KB | 1.3 KB | 00:24:33 |
| 79 | bras.hotspot.service.root | 48.8 MB | 1.7 MB | 01:00:06 |
| 79 | bras.hotspot.service.root | 23.2 MB | 2.3 MB | 02:30:14 |
| 79 | bras.hotspot.service.root | 428.2 KB | 1.5 MB | 00:41:04 |
| 79 | ap.hotspot.service.root | 2.8 MB | 476.2 KB | 00:23:57 |
| 79 | bras.hotspot.service.root | 370.3 MB | 6.7 MB | 06:12:26 |
| 79 | bras.hotspot.service.root | 0 B | 4.8 KB | 00:10:01 |
| 79 | ap.hotspot.service.root | 94.3 MB | 5.9 MB | 00:30:16 |
| 79 | bras.hotspot.service.root | 4.8 MB | 501.5 KB | 00:30:03 |
| 79 | bras.hotspot.service.root | 183.9 MB | 3.8 MB | 00:40:04 |
| 79 | bras.hotspot.service.root | 16.8 MB | 971.1 KB | 00:30:03 |
| 79 | bras.hotspot.service.root | 48.0 MB | 3.3 MB | 01:00:16 |

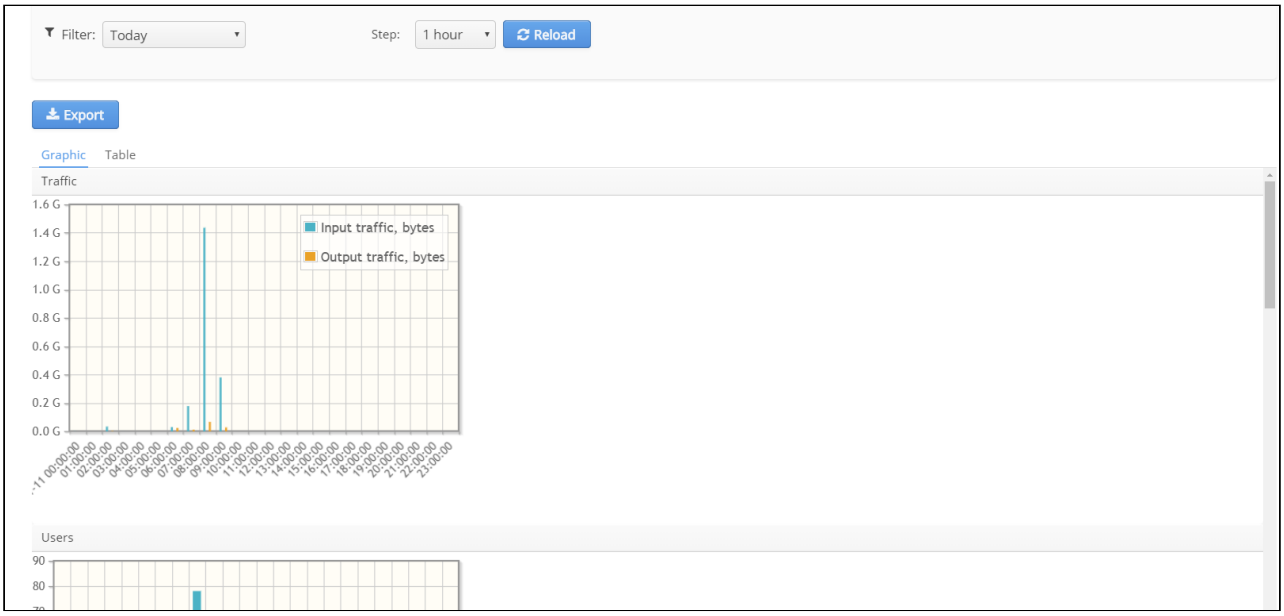
There is a table with user sessions on the tab. The table contains the following tabs:

- Username
- Domain
- Input Octets
- Output Octets
- Session Time

## SSID Groups




| SSID | SSID Domain | Data received | Data sent | Connections | Unique MACs | Unique clients | Active APs |
|---|---|---|---|---|---|---|---|
| BRAS-Guest | | 722.1 KB | 182.9 KB | 11 | 7 | 1 | 1 |
| BRAS-Guest | bras.hotspot.service.root | 779.4 MB | 28.1 MB | 58 | 20 | 19 | 1 |
| Eltex-Guest | ap.hotspot.service.root | 3.6 GB | 172.3 MB | 69 | 23 | 21 | 25 |
| Eltex-Local | enterprise.service.root | 2.2 GB | 144.0 MB | 678 | 103 | 97 | 60 |
| Summary | | 6.5 GB | 344.6 MB | 817 | - | - | - |
| Unique values | | - | - | - | 149 | 137 | 62 |

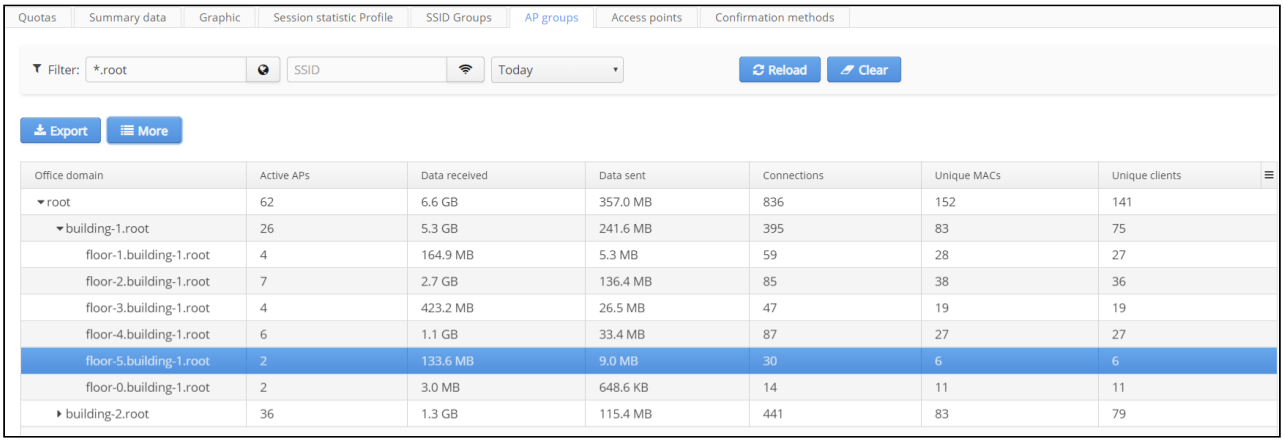


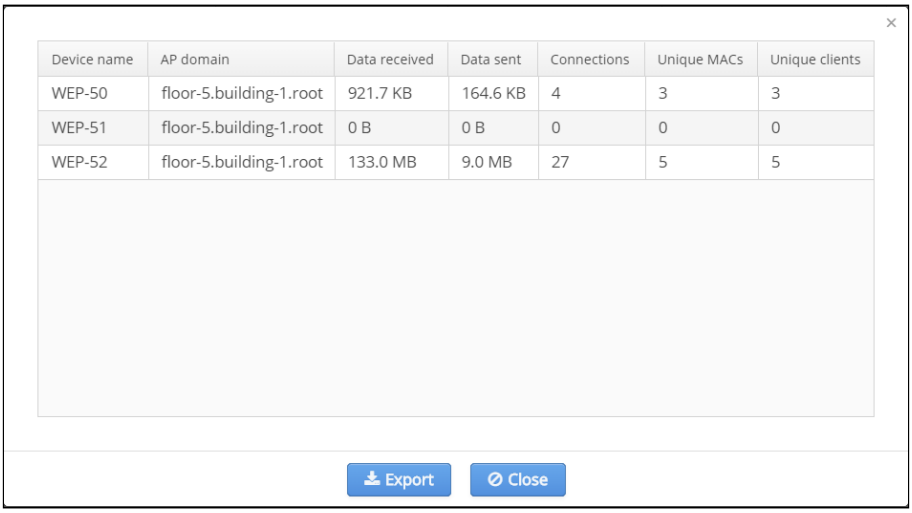

The tab *"SSID Groups"* allows obtaining statistics on the whole network from the perspective of SSID. The tab contains filters on the domain and on the date.The summary table includes the following information:

- SSID;
- SSID Domain;
- Data received, in bytes (for clients of service);
- Data sent, in bytes (for clients of service);
- Connections (to SSID);
- Unique clients (login);
- Unique MACs (devices);
- Active APs (the number of access points really used for providing a service to a corresponding SSID).

The total number of elements is displayed in the row *"Summary"* for the columns for which this parameter has physical sense.The row *"Unique values"* contains the total number of unique values for all SSIDs that satisfy the sampling condition.
The row *"Unique values"* is necessary because some access points have several SSIDs. At the same time, some user devices (MAC) can get a service in several SSIDs. As a consequence, the simple summation of cell values will lead to wrong results.
Statistics can be displayed for each SSID (cell). To view statistics, click on the required row with the left button and then click More . A modal dialog with detailed information will be displayed.

AP groups



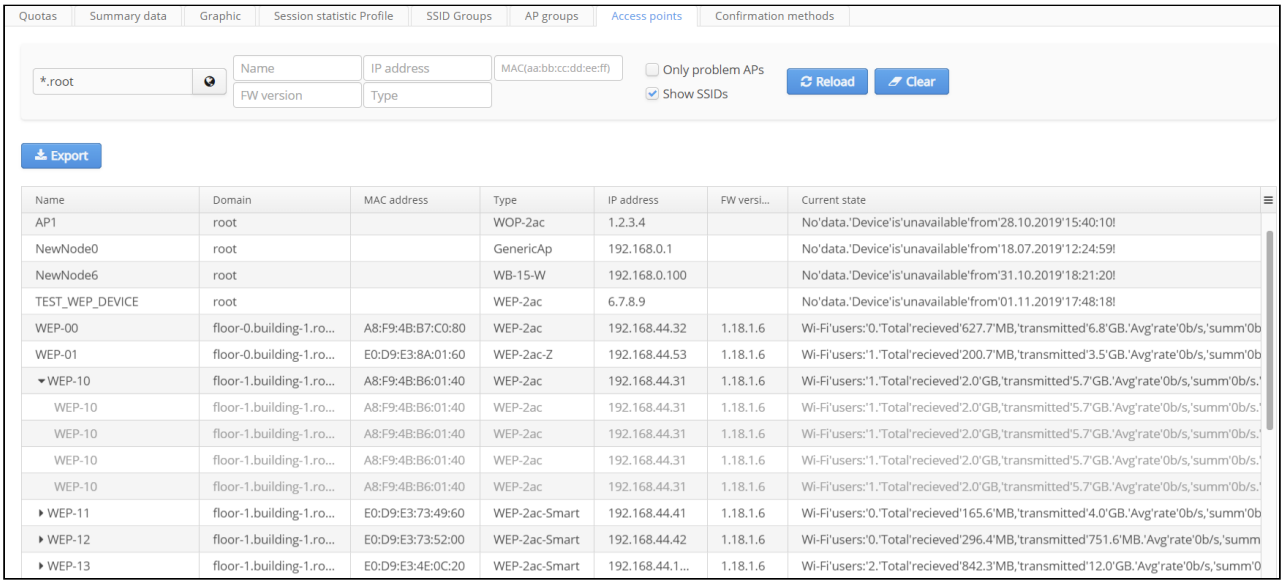



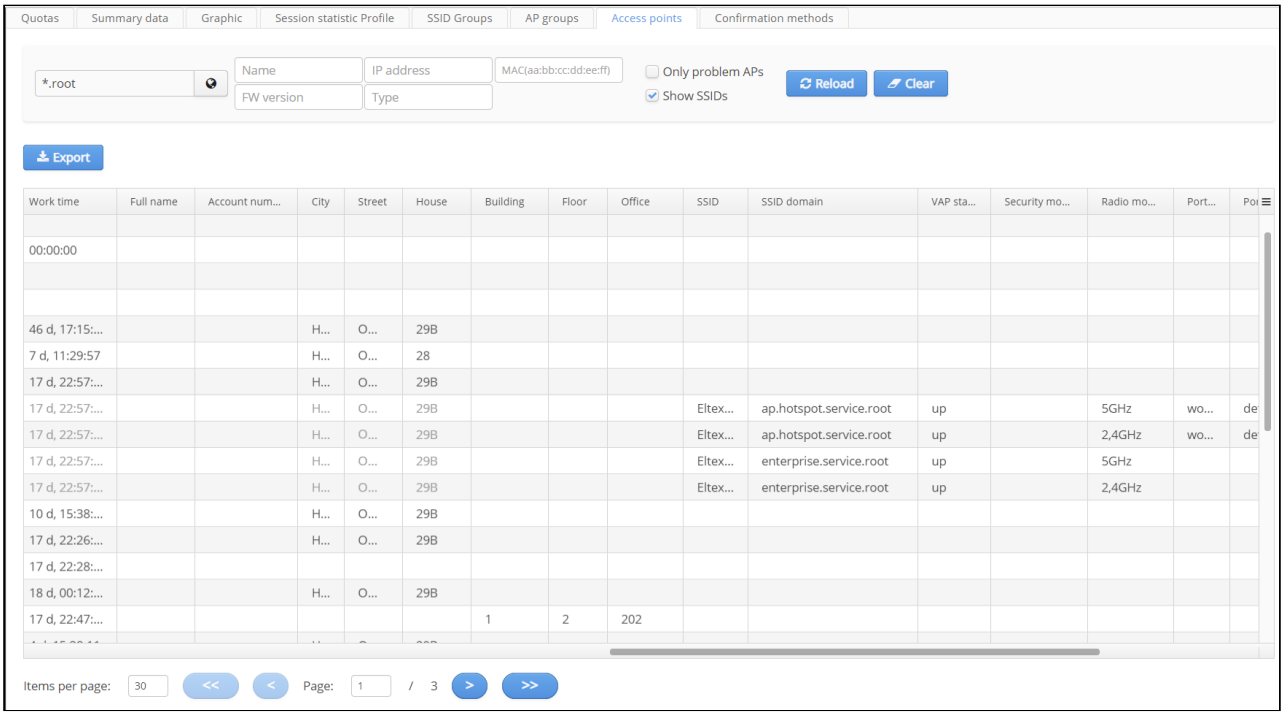

The tab "AP Groups" allows getting statistics on AP groups. Access points are grouped by a domain (i.e. according to organization and location).Information shown for each group:

- Office domain;
- Active APs;
- Data received, bytes (incoming traffic for Wi-Fi users);
- Data sent, bytes (outgoing traffic for Wi-Fi users);
- Connections (for all SSIDs on the AP);
- Unique MACs (the total number of unique subscriber devices served by the AP on all SSIDs);
- Unique clients (the total number of unique user accounts "login" served by the AP on all SSIDs);

To obtain more detailed information on AP clients, select a domain in which access points are located (statistics is not obtained for nested domains) and click the button More .

Access points




The tab "Access points" contains information on status of access points installed in the network.
The following AP parameters are displayed in the table:

- Name
- Domain
- MAC address
- Type
- IP address
- FW version
- Current state:
    - Wi-Fi users

    - Total received (received traffic, MB)
    - Transmitted (sent traffic, GB)
    - Avg and Summ rate (average and summary transfer rate. Kb/s)
- Work time, seconds
- Full name
- Account number
- City Street
- House
- Building Floor
- Office

> The following columns are filled in after activating the checkbox "Show SSIDs". When it is checked, SSIDs and information on them are displayed in corresponding cells of the table for each access point.

- SSID
- SSID domain
- VAP state
- Security mode
- Radio mode
- Portal
- Portal tariffs

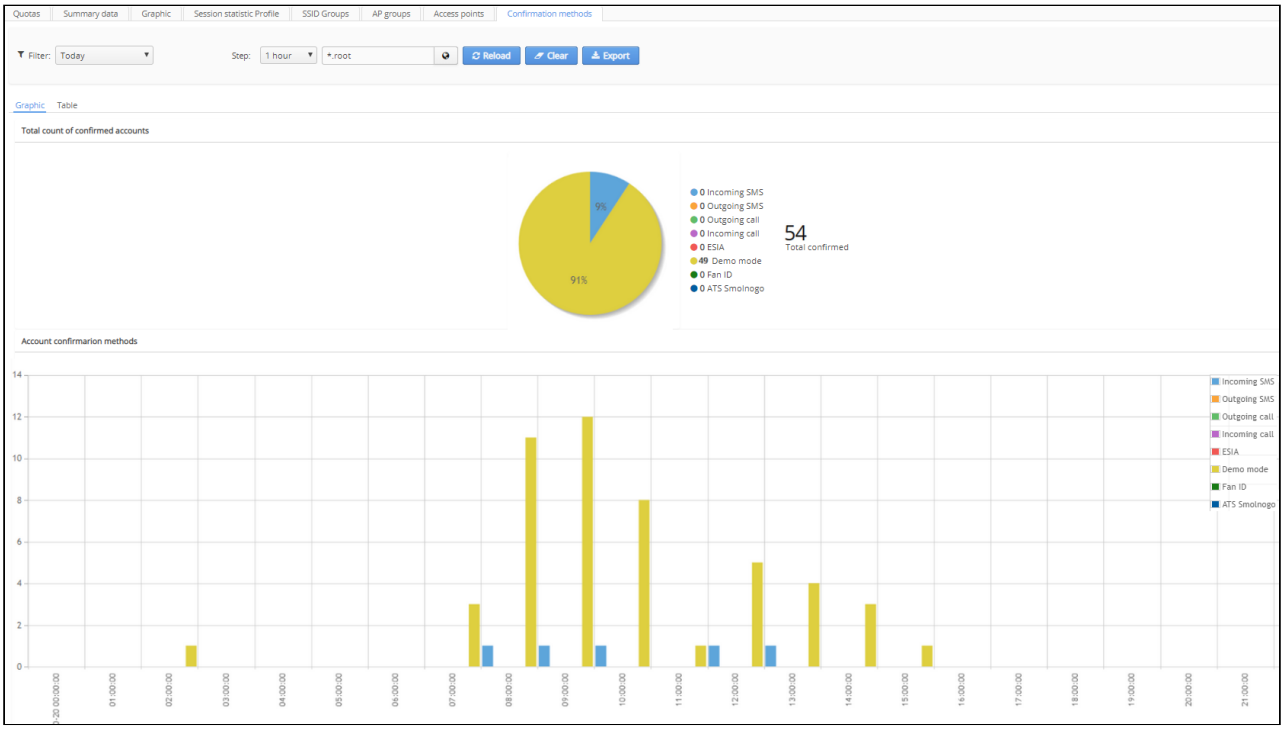
The list of displayed access points can be filtered with the help of the following filters:

- by domain
- by name
- by IP address
- by MAC
- by FW version

When the checkbox "Only problem APs" is checked, access points to which connection was lost can be filtered.

Confirmation methods

---




In this tab, statistics is displayed as charts on subscriber authentication methods (methods of phone numbers confirmation). There are 8 account confirmation methods:

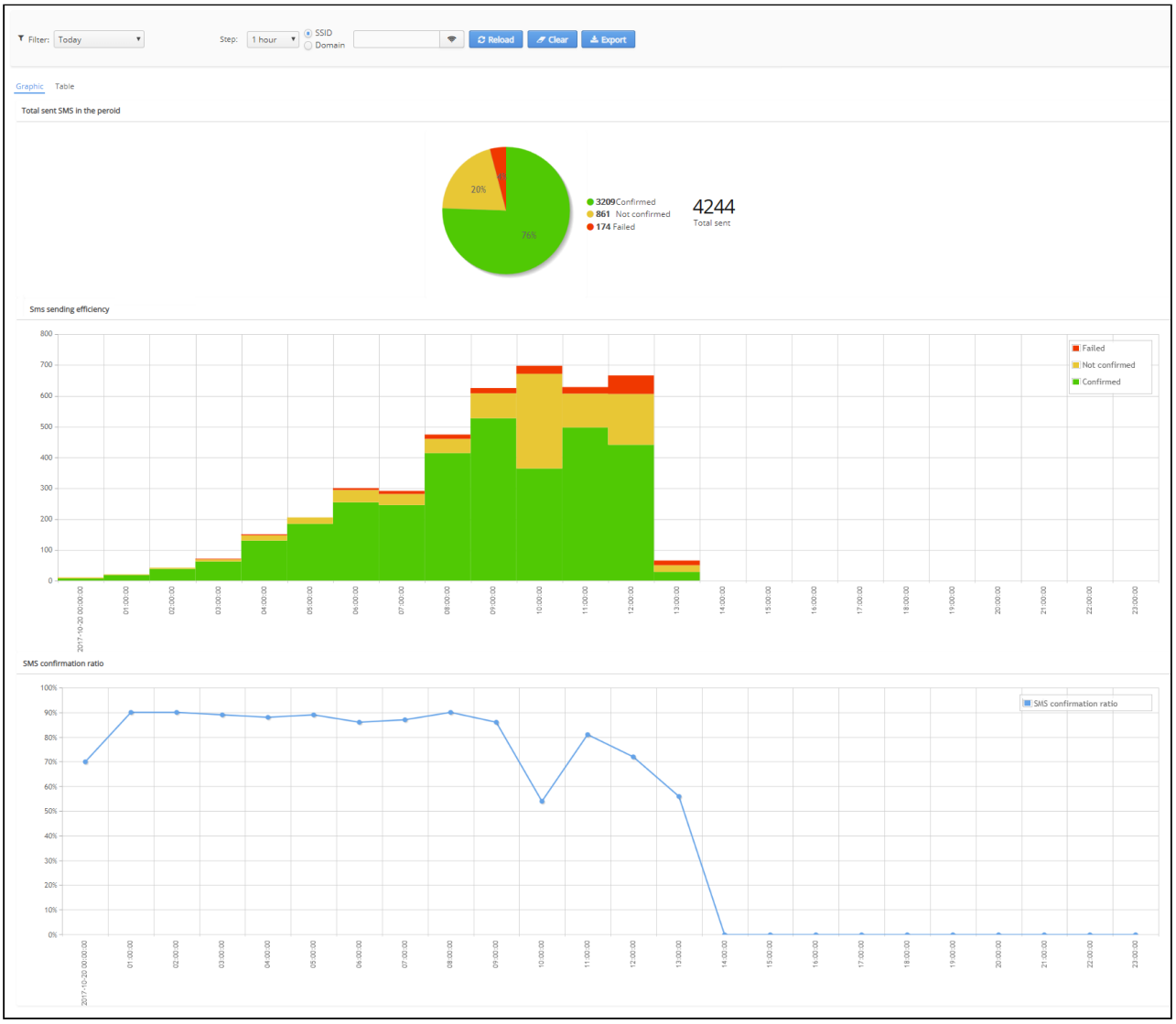
- Incoming SMS
- Outgoing SMS
- Outgoing/Incoming call
- ESIA
- Demo mode
- Fan ID
- ATS Smolnogo

A pie chart showing percentage of account confirmation methods for all time and a bar chart showing distribution of authentication methods during a certain time period can be found on the tab. The same statistics can be also displayed in the tabular form.

## SMS Statistic

In this section, statistics on SMS messages sent to subscribers by the system via an SMS gateway during portal authorization.

### SMS statistic by time

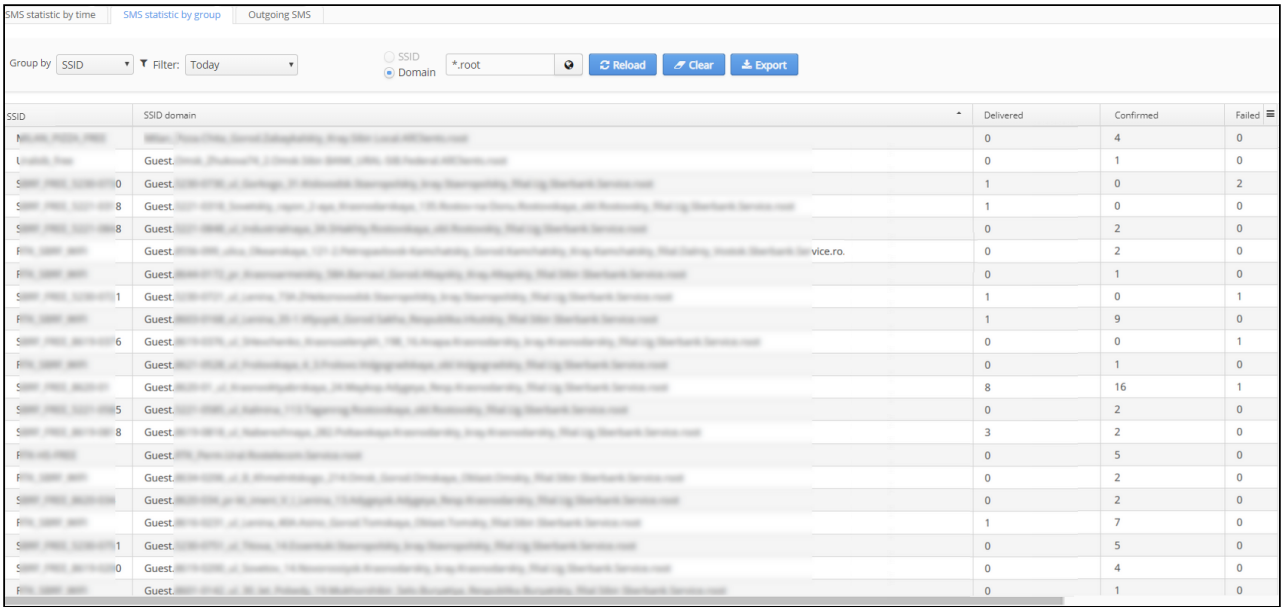



This tab contains charts showing statistics on SMS sent during a certain period of time:

- Total sent SMS in the period (the number of confirmed, not confirmed, failed SMS during the whole period shown as a pie chart)
- SMS sending efficiency (the number of confirmed, not confirmed, failed SMS during the whole period shown as a pie chart)

SMS confirmation ratio (percentage of SMS after sending which a user has confirmed his account and authorized on the portal)
There are filters on the time, the SSID or the domain on the page. If the checkbox "SSID" is selected, it is possible to set a filter on the SSID, if "Domain" is selected, it is possible to set a filter on the domain.

## SMS statistic by group




In this tab, there is a table containing statistics on sent SMS with and opportunity to filter them on:

- SSID
- Time (set by the corresponding checkbox)
- Domain (set by the corresponding checkbox)

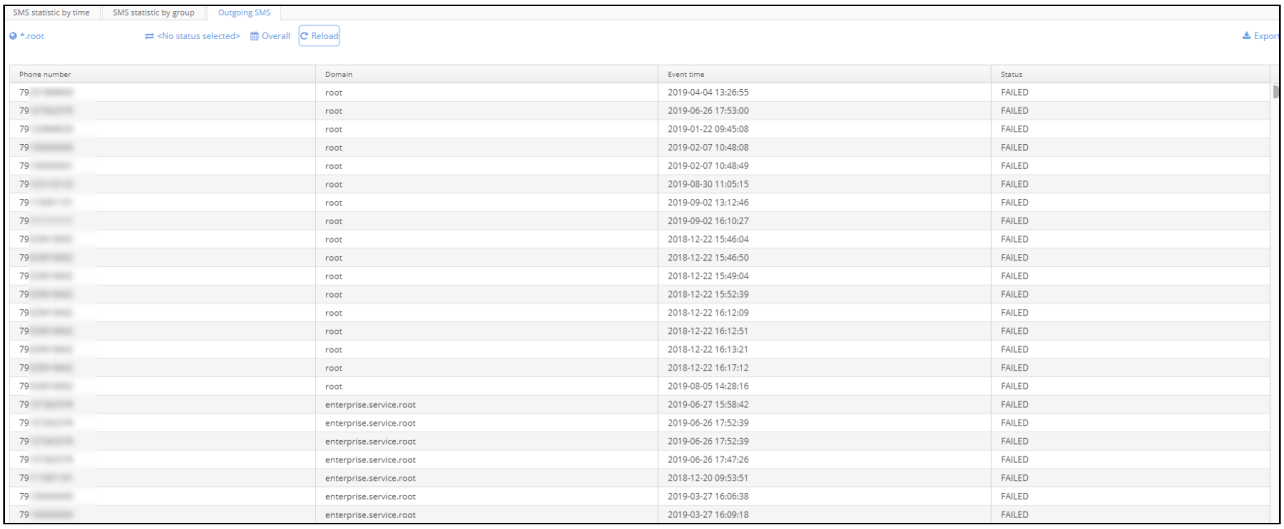
Results displayed in the table can be grouped by:

- SSID
- Domain
- Geodomain
- Portal

The table contains the following information:

- SSID
- SSID domain
- Delivered (the number of SMS delivered to a subscriber)
- Confirmed (the number of SMS after receiving of which a subscriber confirmed his account on the portal)
- Failed (the number of SMS that has not been delivered)

## Outgoing SMS




The table contains a list of all sent SMS. The following data is displayed:

- Phone number (to which an SMS was sent)
- Domain (in which a user is registered)
- Event time (date of sending)
- Status:
    - "SENT" — a message was sent to a gateway, and is accepted for processing.
    - "CONFIRMED" — a message was sent, and a user passed authorization with a temporary password.
    - "FAILED" — an attempt to send a message failed (a gateway denied a request, or a timeout was exceeded).

## Hotspot/Enterprise statistics

The sections contain statistics on authorization, Hotspot - SSID services with portal authorization and Enterprise - SSID services with RADIUS (EAP) authorization.
For users with RADIUS authorization data on traffic and sessions only is displayed. For users with portal authorization data on more parameters is available.

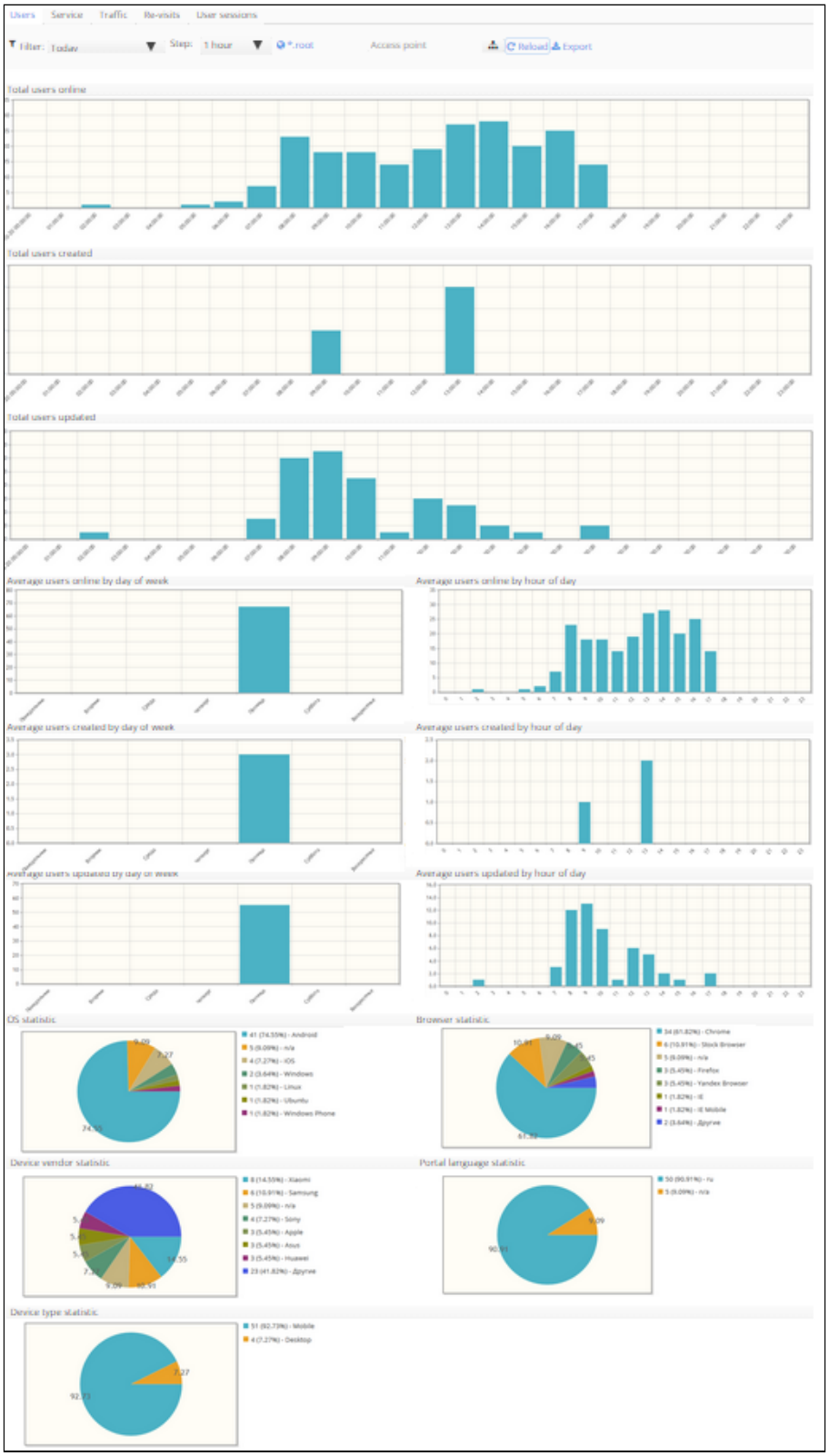
### Control elements


The tabs "Users", "Service", "Traffic" and "Re-visits" have similar control elements.

- Filter — a time period for sampling

- Step — an interval for histogram construction
- Domain — a domain within which data sampling is performed
- Access point — sampling data on a certain access point.
- Reload — read data from a database using new filter settings

Users



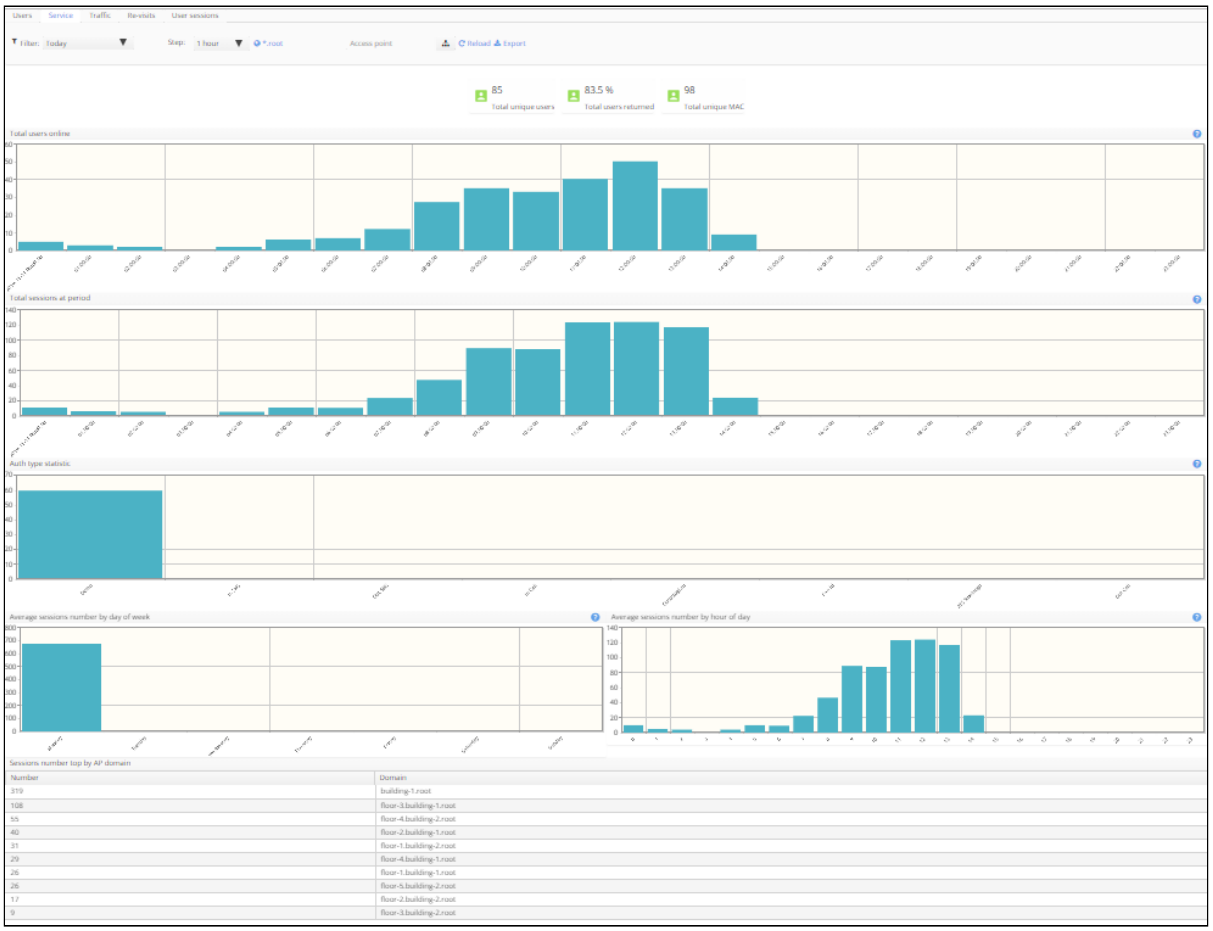

This tab contains the following diagrams:

- Total users online

- Total users created
- Total users updated
- Average users online by day of week
- Average users online by hour of day
- Average users created by day of week
- Average users created by hour of day
- Average users updated by day of week
- Average users updated by hour of day
- OS statistic
- Browser statistic
- Device vendor statistic
- Portal language statistic
- Device type statistic

Data filtering by the time and the domain is available.

## Service

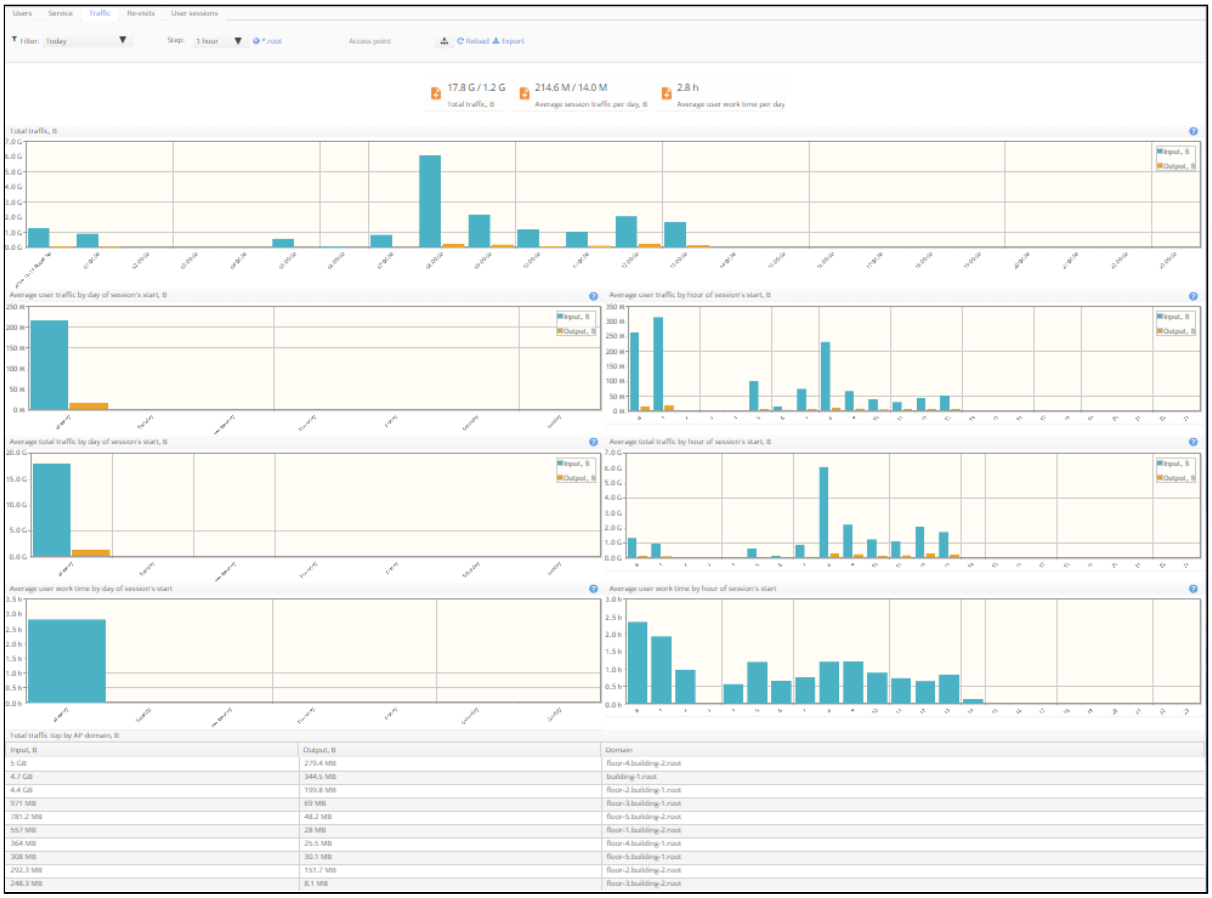


This tab contains the following diagrams:

- Total users online
- Total sessions at period
- Auth type statistic
- Average sessions number by day of week
- Average sessions number by hour of day
- The table "Sessions number top by AP domain" The table contains:
    - Domains
    - Number of sessions in each domain

Data filtering by the time and the domain is available.

## Traffic (Hotspot/Enterprise)



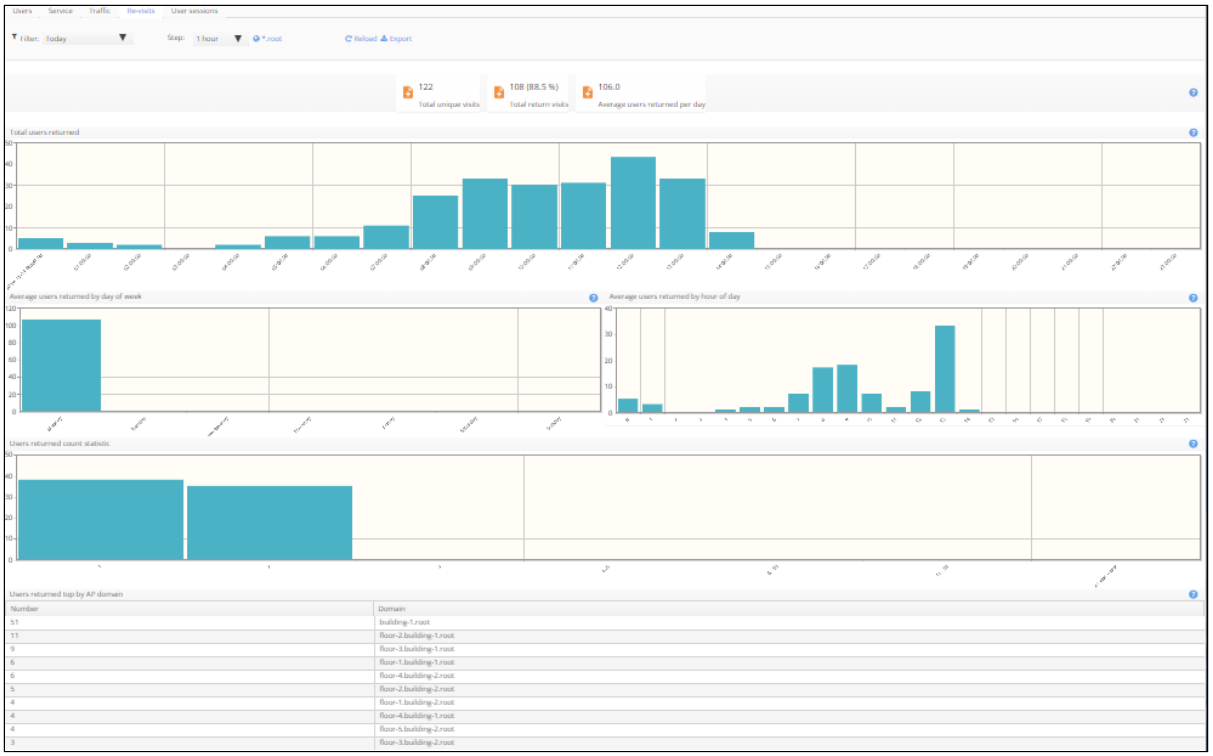
This tab contains the following diagrams:

- Total traffic
- Average user traffic by day of session's start
- Average user traffic by hour of session's start

- Average total traffic by hour of session's start
- Average total traffic by hour of session's start
- Average user work time by day of session's start
- Average user work time by hour of session's start
- The table "Total traffic top by AP domain"

Data filtering by the time and the domain is available.

## Re-visits

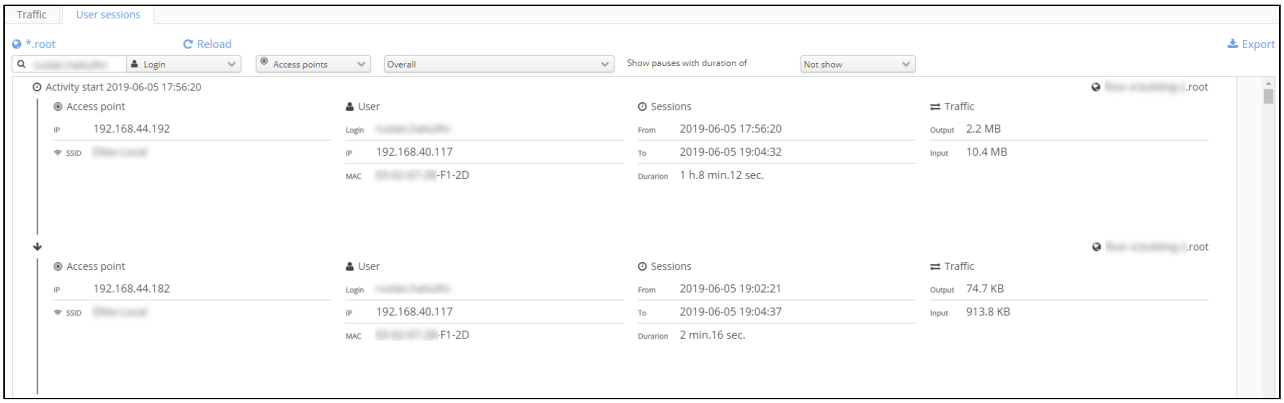


This tab contains the following diagrams:

- Total users returned
- Average users returned by day of week
- Average users returned by hour of day
- Users returned count statistic
- The table "Users returned top by AP domain"

Data filtering by the time and the domain is available.

## User sessions (Hotspot/Enterprise)




The table is intended to display data on Wi-Fi users' sessions and allows tracking users' movements with the time of their connection to access points and disconnection from them.
Displayed data:

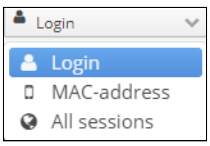
- Domain
- Access points
    - IP
    - SSID
- User
    - Login
    - IP
    - MAC
- Sessions
    - From
    - To
- Traffic
    - Input
    - Output

Standard control elements:

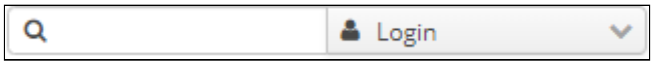
- **Domain** — define a domain within which a search for sessions will be carried out.
- **Reload** — make a request to a database again to reflect filter changes.
- **Export** — export obtained data to .csv.

The table also has a special set of filters and display modes.

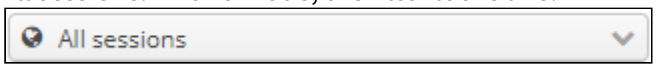
Searching for user sessions




There are several modes to search user sessions:

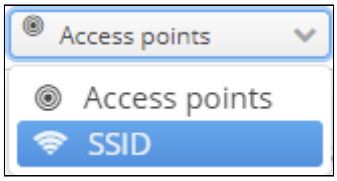
- By login. In this mode, the filter looks like: 

. A search for an expression specified in the field will be performed.
- By MAC address. In this mode, the filter looks like:


. A search will be performed on MAC address specified as hexadecimal numbers divided by colons.
- All sessions.  In this mode, the filter looks like:


. In this mode, all sessions from a domain specified in the filter will be displayed.

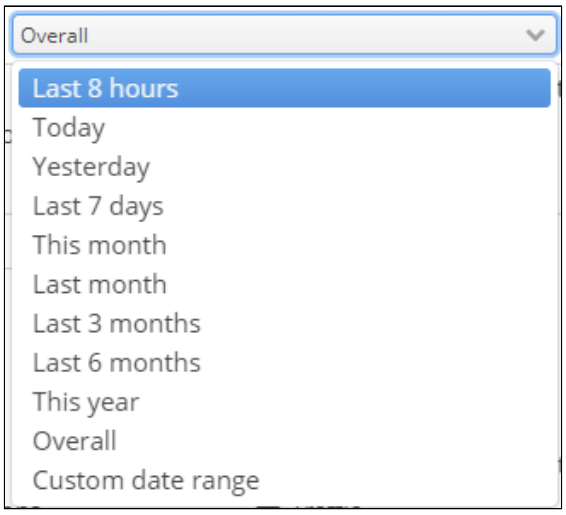
Grouping mode




The following modes of grouping the results are available:

- **Access points** — user sessions will be grouped by access points. This mode should be used if it is necessary to obtain exact information on what access points a user connected to.
- **SSID** — sessions will be grouped by SSID. In this mode information on SSIDs to which a user was connected is given.

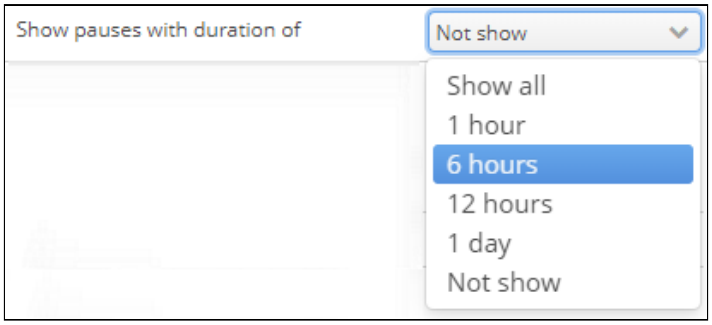
Sampling dates range




Specifying a time range for which a search will be performed. Select one of the proposed time templates:

Or specify a required interval by selecting "Custom date range":


### Merging sessions

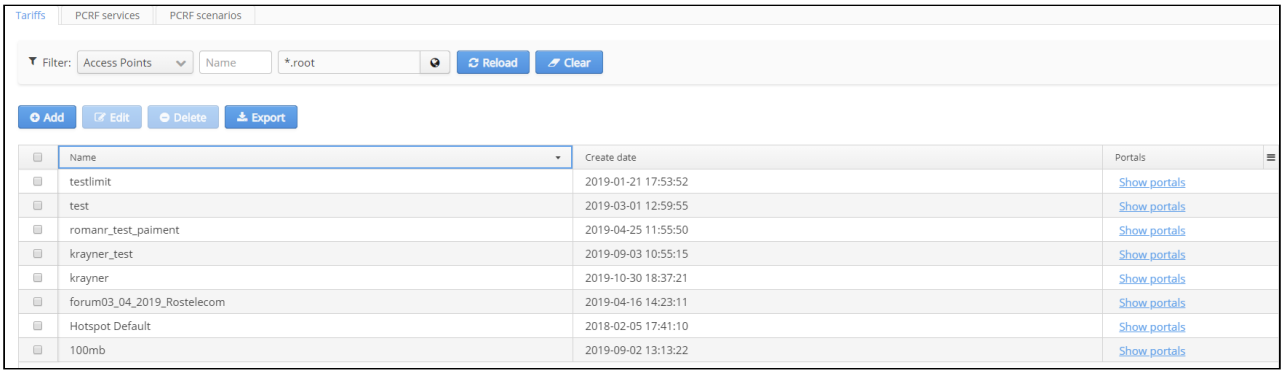



Each user session starts with authorization and ends with disconnection from an access point. However, connection and disconnection processes may occur frequently and often invisibly for users, for example when a device enters a sleeping mode to save energy and then returns back. A new session is created during any such cycle. For data to be displayed in the table in a readable form, it is possible to merge several sessions created by the same user on the same access point and SSID into one session if their time interval is lower than some threshold. To configure this option, the parameter "Show pauses with duration of" is used.
One of the following modes can be selected:

- **Show all** — each session will be displayed separately.
- **1 hour, 6 hours, 12 hours, 1 day** — an interval between sessions upon exceeding of which sessions are not grouped.
- **Not show** — merge all user sessions on one access point and one SSID.

## Services and tariffs

### Tariffs




In this section, tariffs for Wi-Fi users' access to the network are configured.
Tariffs are splitted into the two groups:

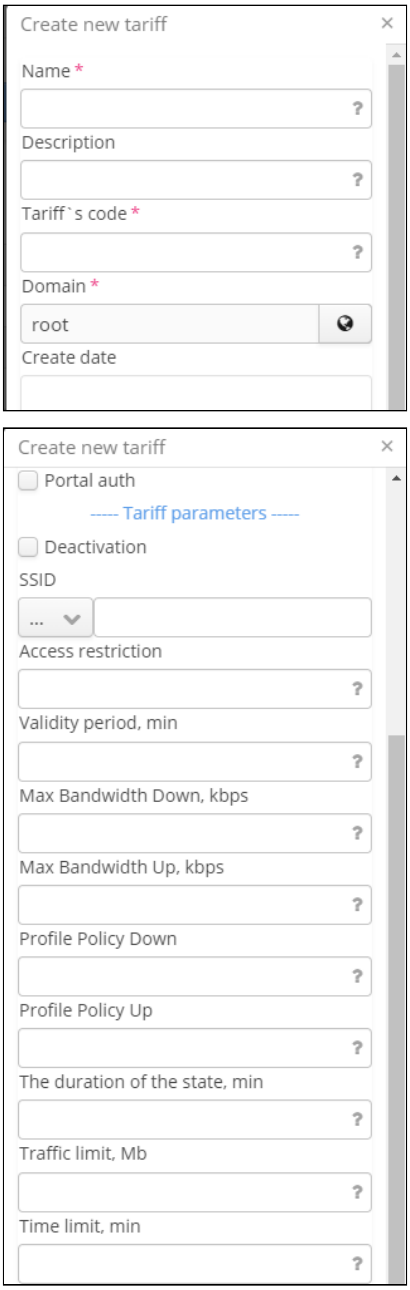
- PCRF/BRAS — authorization is carried out on BRAS with any vendors' access points.
- Access points — authorization is made on Eltex access points. Access points tariffs are in turn splitted into:
    - Enterprise access points — for RADIUS authorization
    - Portal authorization — for authorization via Eltex Portal

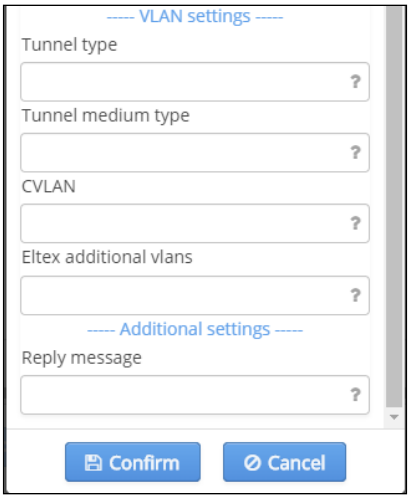
In the tab "Tariffs" there is a table with the following fields:

- Name — tariff name
- Code — unique tariff code
- Domain — tariff domain
- Create date — date of tariff creation
- Description — tariff description in free-form text
- Users — user accounts related to a tariff under consideration
- Portals — portals related to a tariff under consideration (if this column is not displayed, enable it via table properties by clicking a button in the upper right corner of the table).

Tariffs for access points

Enterprise tariffs

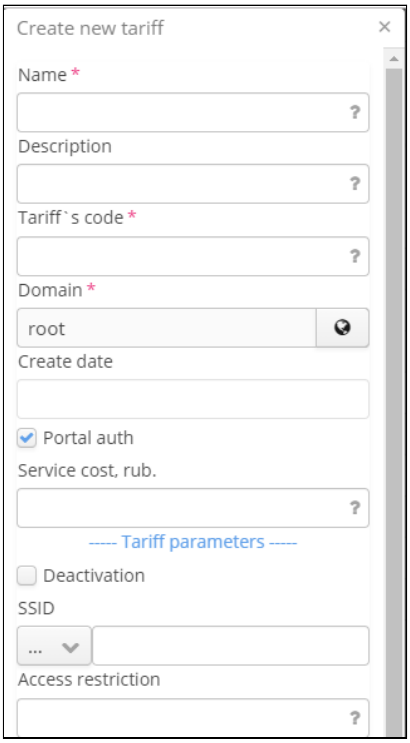

Create new tariff
Name *
Description
Tariff`s code *
Domain *
root
Create date
Create new tariff
Portal auth
----- Tariff parameters -----
Deactivation
SSID
...
Access restriction
Validity period, min
Max Bandwidth Down, kbps
Max Bandwidth Up, kbps
Profile Policy Down
Profile Policy Up
The duration of the state, min
Traffic limit, Mb
Time limit, min

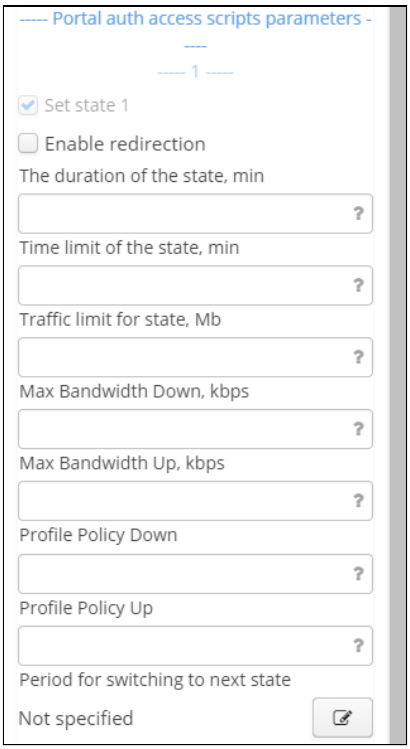


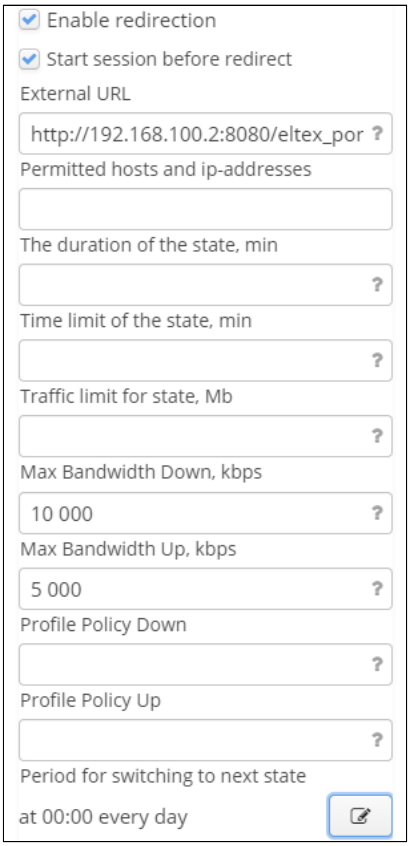

Enterprise tariffs are used to specify limitations for sessions of users authorized via RADIUS in WPA-enterprise mode.

- Name – tariff name;
- Description – tariff description;
- Tariff's code – tariff code;
- Domain – tariff domain;
- Create date – tariff creation date (set automatically);
- Deactivation – disable authorization of users with a certain tariff and user account until this account and relevant statistics is removed from a database;
- SSID – name of a Wi-Fi network to which a user will be able to connect;
- Access restriction – the number of client devices that can be authorized under the same account;
- *Max Bandwidth Down/Up, kbps* – downstream and upstream transfer rate limitation for a user;
- *Profile Policy Down/Up* – Policy profile for a certain user. Policy profile is created in the Client QoS menu of an access point;
- *The duration of the state, min* – user session duration;
- *Traffic limit, MB* – downstream traffic limitation for a user;
- *Time limit, min* – time limitation for all user sessions;
- *Validity period* – the period of time during which a user account will be accepted. The period of time is calculated from an account creation date;
- CVLAN for transmitting user traffic to operator network via a separate VLAN (the attributes *Tunnel-Type* and *Tunnel-Medium-Type* with default values "13" and "6" respectively should be enabled).

Tariffs for portal authorization using Eltex access points


Create new tariff
Name *
Description
Tariff`s code *
Domain *
root
Create date
Portal auth
Service cost, rub.
----- Tariff parameters -----
Deactivation
SSID
...
Access restriction


----- Portal auth access scripts parameters -----
----- 1 -----
Set state 1
Enable redirection
The duration of the state, min
Time limit of the state, min
Traffic limit for state, Mb
Max Bandwidth Down, kbps
Max Bandwidth Up, kbps
Profile Policy Down
Profile Policy Up
Period for switching to next state
Not specified

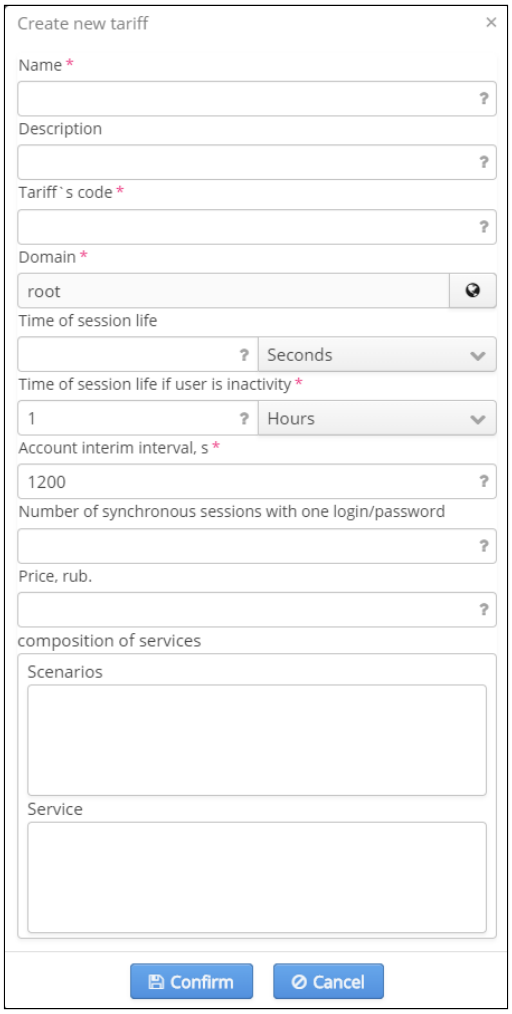



- Tariffs of this type relate to creating access scenarios for users registered via Eltex access points with portal authorization configured. A tariff can have several access scenarios according to which a user is given full or limited Internet access.
- Name – tariff name;
- Description – tariff description;
- Tariff's code – tariff code;
- Domain – tariff domain;
- Create date – tariff creation date (set automatically);
- Price – the cost of using a certain tariff;
- Deactivation – disable authorization of users with a certain tariff and user account until this account and relevant statistics is removed from a database;
- SSID – name of a Wi-Fi network to which a user will be able to connect;
- Access restriction – the number of client devices that can be authorized under the same account;

- *Validity period* – the period of time during which a user account will be accepted. The period of time is calculated from an account creation date;
- *Set state N* – enable state N (the first one is always enabled by default);
- *External URL* – URL address for user redirection after portal registration;
- *Start session before redirect* — when the checkbox is set, a session starts before redirection to an external URL address;
- *The duration of the state* — the maximum duration of state N in minutes;
- *Time quota of the state* — common quota for all user sessions within state N in minutes;
- *Traffic quota of the state* — common quota for user downstream traffic within state N in megabytes;

- *Max Bandwidth Down/Up, kbps* — bandwidth limit for user downstream and upstream traffic within state N in kbps;
- *Profile Policy Down/Up* — Policy profile for a certain downstream user within state N;
- *Permitted hosts and IP addresses* – the list of dns and IP addresses that are accessible without portal authorization. Permitted addresses should be separated by a comma.
- *Period for switching to next state* — a cron expression at which the switch to a next state happens.

PCRF/BRAS

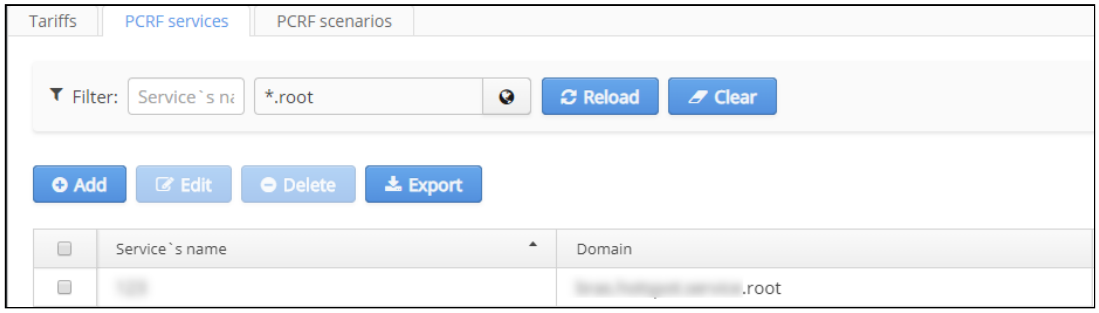


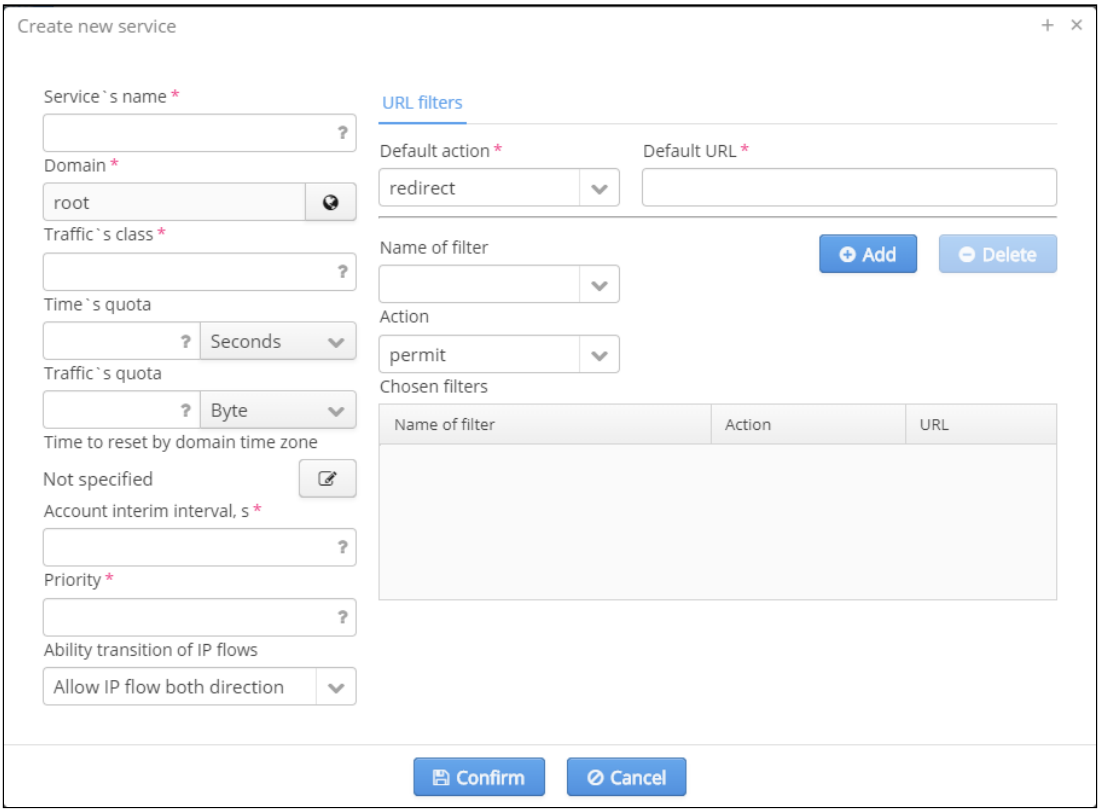

Tariffs of this type define rules according to which a user with portal authorization will act in the scheme with BRAS

- *Name* — an arbitrary name;
- *Description* — a tariff description;
- *Tariff's code* — a tariff unique identifier;
- *Domain* — a domain in which a tariff will be created;

- *Time of session life* — session lifetime;
- *Time of session life if a user is inactive* — session lifetime when idle;
- *Composition of services* — the set of available scenarios and services.

PCRF services

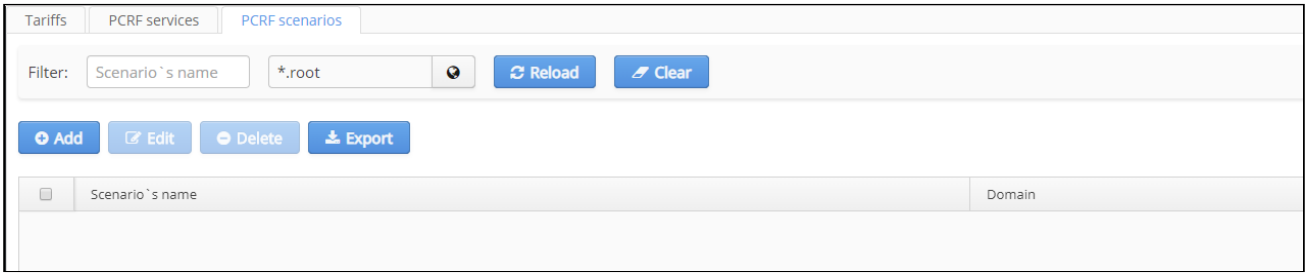


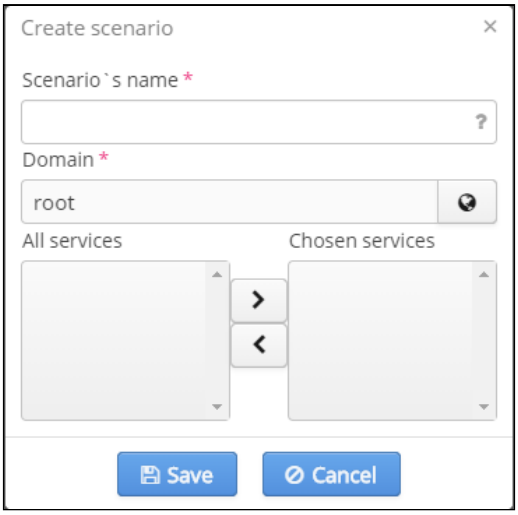




*Service* — a policy applied to a user. For PCRF services to work in service router configuration, relevant access control lists (ACL) should be created. ACL name should be consistent with traffic class in service configuration. WELCOME service is used for user re-authorization. This service is obligatory, and it should be located in the root domain.

- *Service's name* — an arbitrary name that should not match a scenario's name;
- *Domain* — a domain in which a service will be located;
- *Time's quota* — time during which a service will work;
- *Traffic's quota* — volume of traffic available for a user;
- *Account interim interval* — interval between account information updating (radius interim-update);
- *Ability transition of IP flows* — approval or prohibition on traffic transmission in some direction;
- *Default action* — an action that will be applied to the service. The parameter can accept values: permit, deny, redirect;
- *Default URL* — a URL to which a user will be redirected when "redirect" action is selected. A URL should be specified in the filter with "permit" action;
- *Name of filter* — a filter that allows or denies access to a URL. For each filter a URL list should be specified. Each service may have up to 4 filters;
- *Action* — an action applied to a filter. Can accept values: permit, deny, redirect, redirect-without-parameters (no information needed in the field "URL" for redirection);
- *URL* — a URL to which a user will be redirected when the action redirect or redirect-without-parameters is selected.

PCRF scenarios




Scenario — a set of services merged into one entity. The reserved word "again" is used for a scenario to move back to the first step. For example, a scenario consists of INTERNET, LAN, again. When connected, a user will get the service INTERNET, then move to LAN. After that, a user will return to INTERNET on again

command, then move to LAN etc. To use scenarios, a corresponding license is required.

- Scenario's name — an arbitrary name that should not match a service's name;
- Domain — a domain in which a scenario will be located;
- All services - the list of all services;
- Chosen services — the list of selected services.

### Wi-Fi users

The section *"Wi-Fi users"*allows viewing and editing Wi-Fi users lists. The section has three subsections (tabs) that allow working with different groups of service recipients independently.

Each tab has structure similar to other tabs but differs from them in some specific control elements.

At the top of pages filters and control buttons are located. Under them a table containing information on Wi-Fi users can be found. The common elements are: a filter bar, buttons for creating/removing entries and a table with user accounts.

Each user account should have a set of mandatory attributes and a set of optional attributes. Mandatory attributes are:

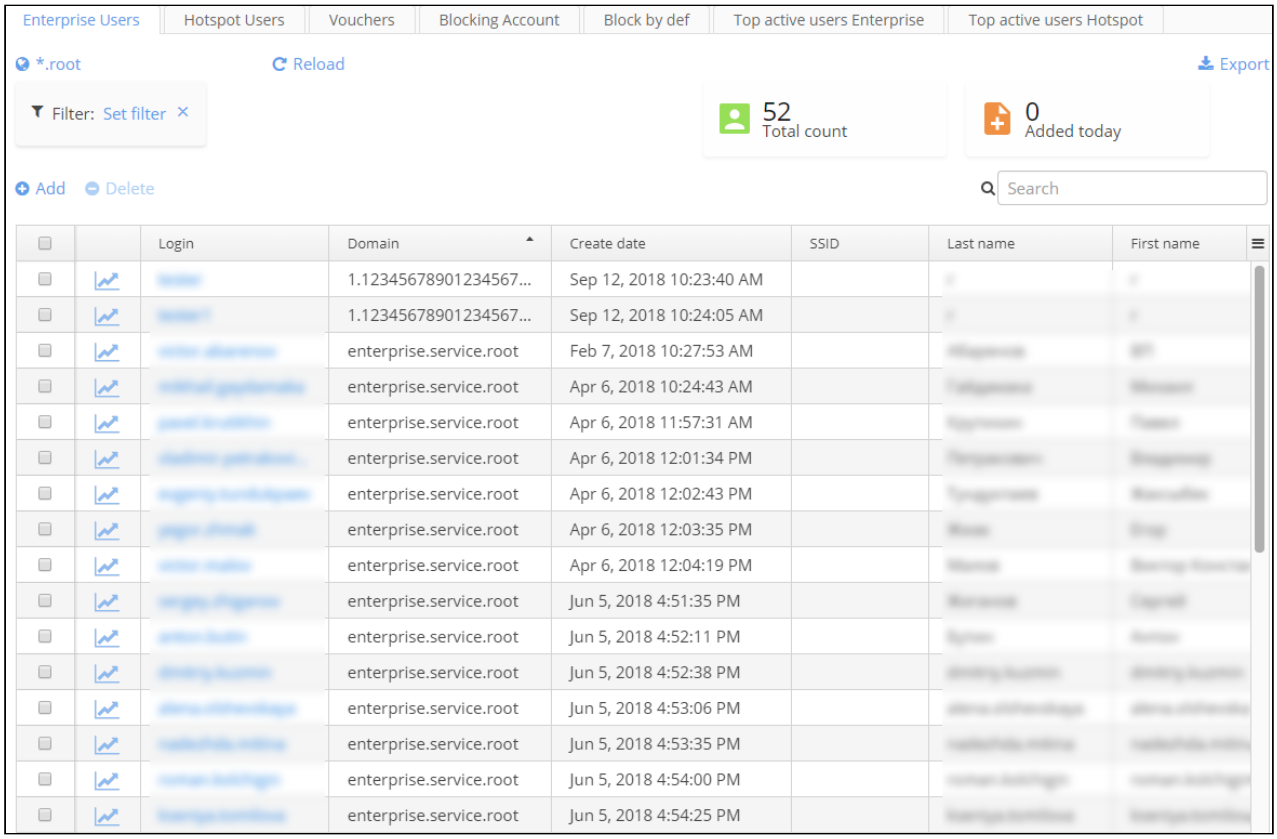
- login;
- password;
- domain.

Other attributes are optional and can be ignored when an entry is created. A set of optional attributes depends on user account type.

There are three types of user accounts in the Wi-Fi Platform:

- Enterprise;
- Hotspot;
- Vouchers.

#### Enterprise

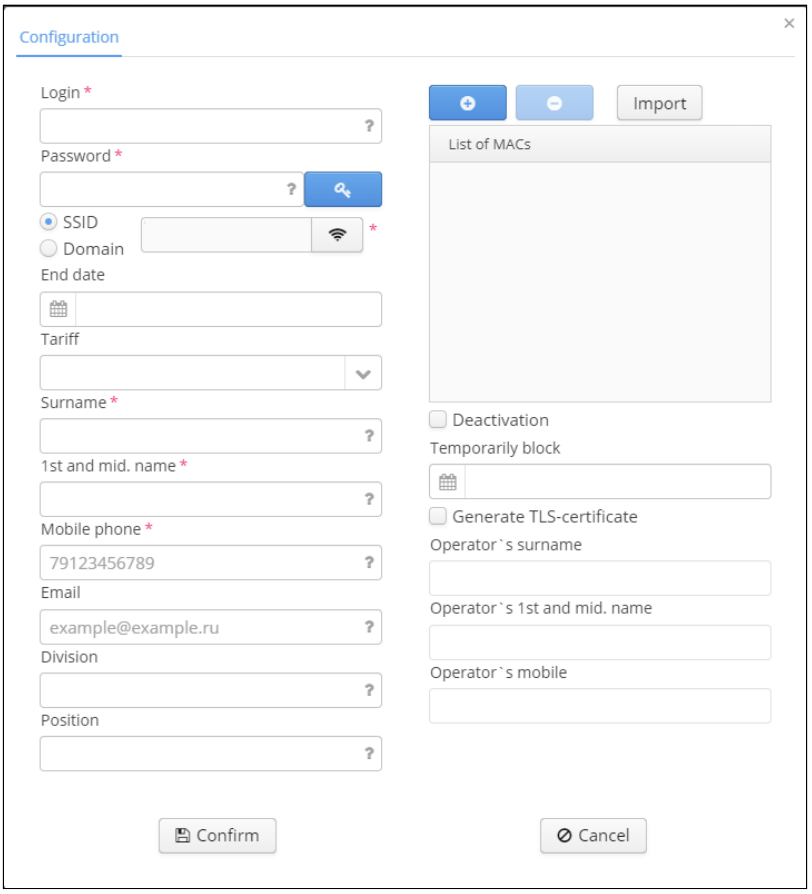


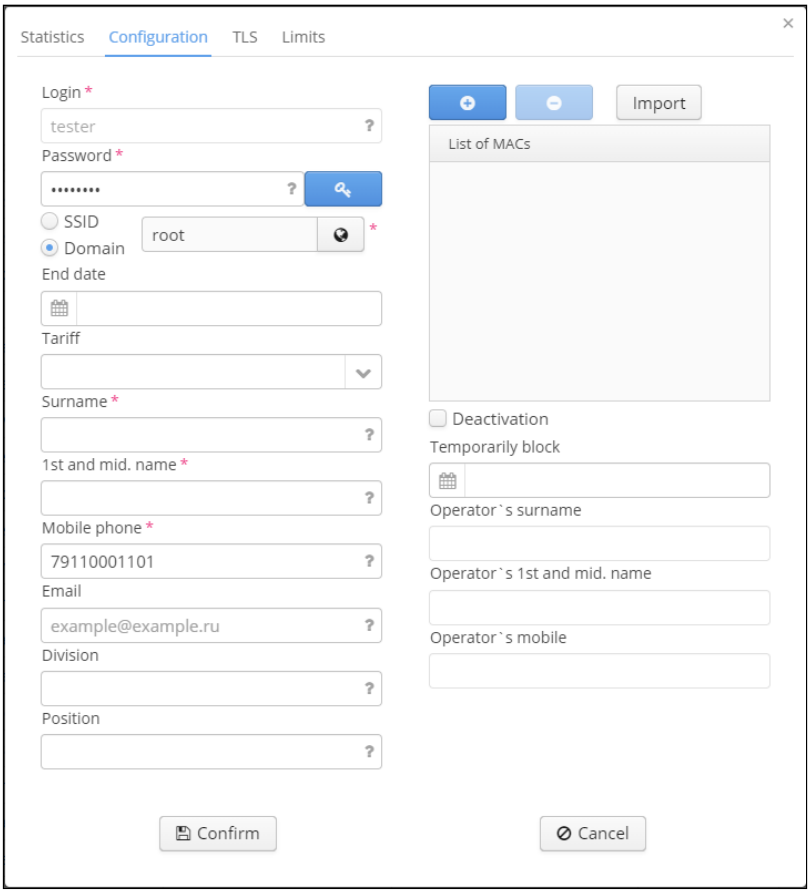

This tab is intended for creating user accounts that will receive logins and passwords for authorization in secure enterprise networks. Such user accounts are usually created for all company employees having access to Wi-Fi. Each user account has a login, a password and several optional parameters. A list of MAC addresses from which an enterprise user can enter an enterprise network can be specified too.

### Entries filtering

Entries can be filtered by login, tariff or user status.

### Adding and editing an entry


Configuration
Login *
Password *
SSID
Domain
End date
Tariff
Surname *
1st and mid. name *
Mobile phone *
79123456789
Email
example@example.ru
Division
Position
Import
List of MACs
Deactivation
Temporarily block
Generate TLS-certificate
Operator`s surname
Operator`s 1st and mid. name
Operator`s mobile
Confirm
Cancel



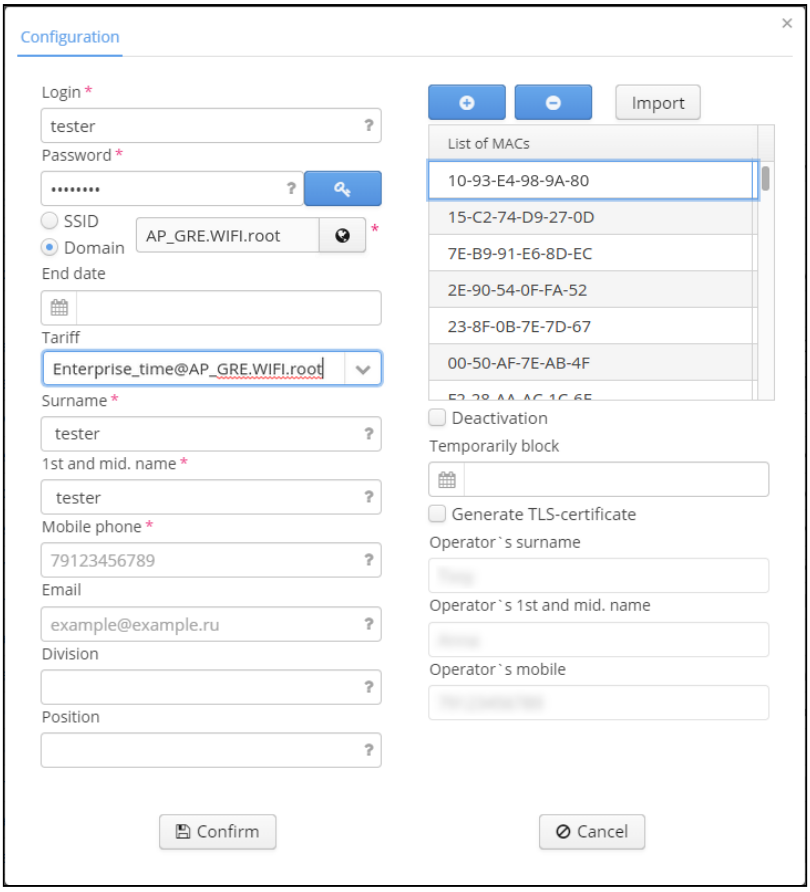

When the button *"Add"* is clicked, an edit window containing a fixed set of parameters is opened. Fields marked with "*" are obligatory. An attempt to save an entry with empty or incorrectly filled obligatory fields will be rejected. Empty or incorrectly filled fields are highlighted in red. When a mouse is moved over a field, a tip with rules on completing this field is displayed.The fields "Login", "Domain" and "Password" are obligatory in all scenarios. Other fields are optional in basic configuration. If it is necessary to make an optional field obligatory to be filled in, an administrator of the Wi-Fi B2B Admin Panel should specify it in system settings .User account parameters:

- Login (obligatory);
- Password (obligatory);
- Domain (obligatory);
- End date;
- Tariff;
- Surname;
- 1st and mid.name;
- Mobile phone;
- E-mail;
- Division;
- Position;
- MAC address;
- Deactivation;

The following control buttons are available in user account configuration window:

- *Create a password* – generate a user password according to rules of password generation specified in the menu *"Settings"*;
- *Confirm* – create an entry and save the changes;
- *Cancel* — cancel the changes.

When an account is added, an operator's full name and phone number are registered. Data is taken from an operator's account. If data is not completed, adding an entry is not allowed.
To view and edit an account, click on the name of a corresponding entry. A window containing 3 sections will be opened. The main tab is "Configuration". Here the elements edited during account creating are available for editing too (see above). When an account is added, an operator's full name and phone number are registered. Data is taken from an operator's account. Data should be completed.

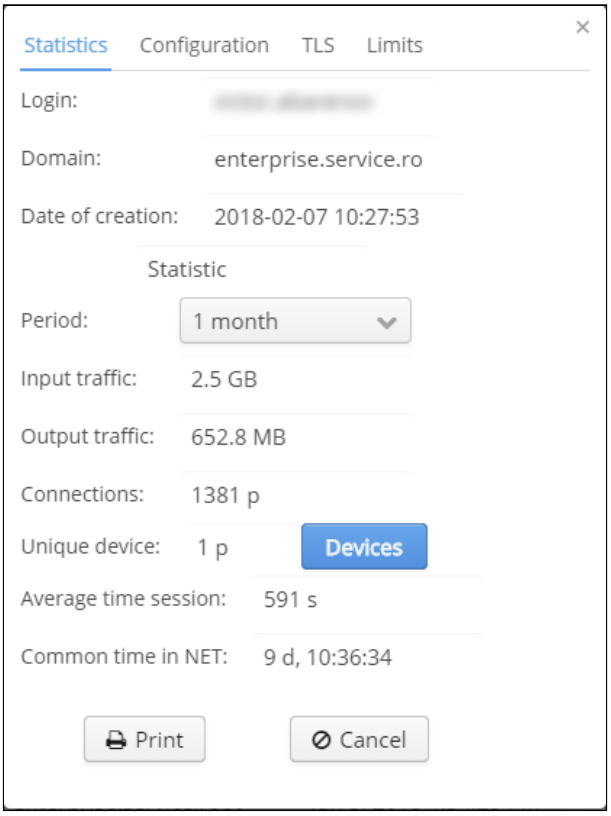


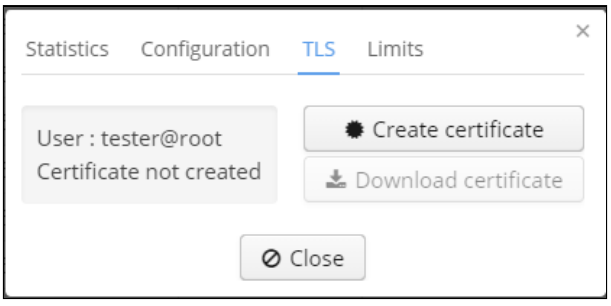

Up to 50 MAC addresses can be assigned to each WPA enterprise account. A MAC address list serves as a white list: Only MAC addresses specified in the list will be able to enter under an account.

To add a MAC address, click the icon "plus" and enter an address in the highlighted field of "List of MACs". To add the following MAC address, repeat the same actions or specify a list consisting of several MAC addresses. To do this, click "Import" and specify a pre-defined list.

MAC addresses should be specified as follows: "00-12-34-56-78-ab". To import a list, format it in advance and specify all MAC addresses in the following form: "00-12-34-56-78-ab".

Viewing statistics and getting a TLS certificate




In the tab "Statistics", basic statistics on an account under consideration is located. The following parameters can be set:

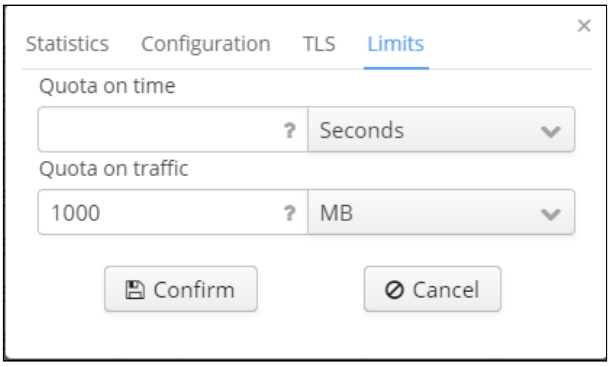
- Period (a time period for which statistics is displayed)
- Input traffic, B

- Output traffic, B
- Connections
- Unique device (the number of unique devices that used an account under consideration)
- A list of devices that used an account under consideration
- Average time session, s
- Common time in NET (total time spent by users on the network under an account considered)
- There is an opportunity to download statistics in PDF format for print (the button "Print")

In the tab "TLS" a TLS certificate for a user can be created and downloaded

Viewing and changing quotas

---




In the tab "Limits" information on time and traffic quotas is displayed. There is an opportunity to edit both time and traffic quota.
Available measurement units for "Time quota":

- Seconds
- Minutes
- Hours
- Days
- Years

Available measurement units for "Traffic quota":

- Byte
- kB
- MB
- GB
- TB
- PB

Deleting entries

To delete an entry, check a corresponding checkbox and click *"Delete"*.

It is possible to delete several entries at the same time.

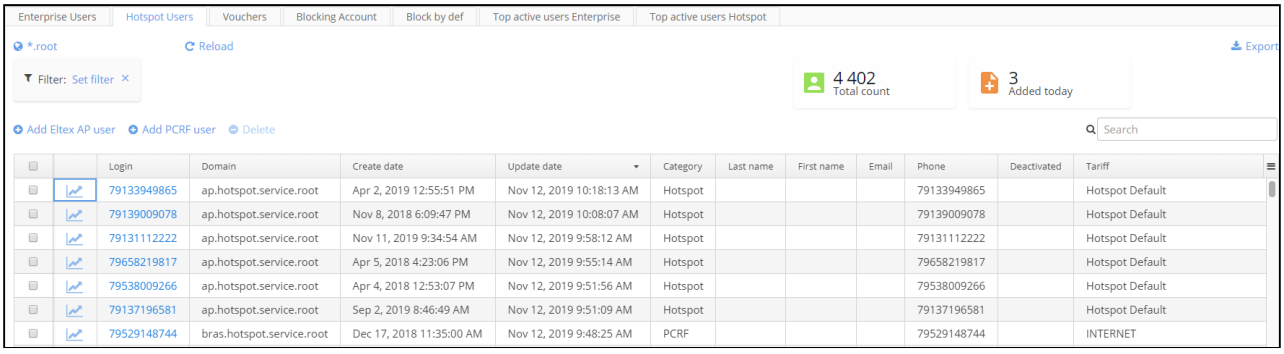
Hotspot users

The interface *"Hotspot users"* for user accounts monitoring is similar to the interface of the tab *"Enterprise users"*. The main difference between the tabs *"Hotspot users"* and *"Enterprise users"* is that types of accounts they work with are different. Although they are similar, one type of accounts is used in private enterprise networks (usually WPA2 Enterprise), and another one is used in networks with portal authorization (Open SSID + Captive Portal).The tab *"Hotspot users"* can be used when providing guest access to an open network with portal authorization.

Guest self-registration on the portal

When enterprise guests perform authorization on the Platform portal themselves (for example, using SMS confirmation), administration do not need to edit such accounts. Although these interface elements are available, it is not recommended to perform any modifications. In this scenario, the tab is used as an element for monitoring and gathering information on users for marketing purposes. For example, exporting a file with users' e-mail addresses. It is permissible if a service agreement says that an organization providing Wi-Fi can officially use data for marketing purposes. To encourage users to enter e-mail, a corresponding field on the Platform portal can be made obligatory.

**User accounts prior creation**




When enterprise guests should be authorized on the portal, but self-registration is prohibited (there is such a mode on the portal) it is necessary to create user accounts manually. In this case, staff that creates user accounts should perform actions for the tab *"Enterprise"*. The tab *"Hotspot users"* is used to create users for two scenarios:

- Registration on the Hotspot portal via "Eltex" access points. User accounts have the following set of parameters:
  - Login (obligatory). Field format: length from 1 to 50, only Latin symbols, lowercase and uppercase characters, digits, special symbols: '_', '.', '-';

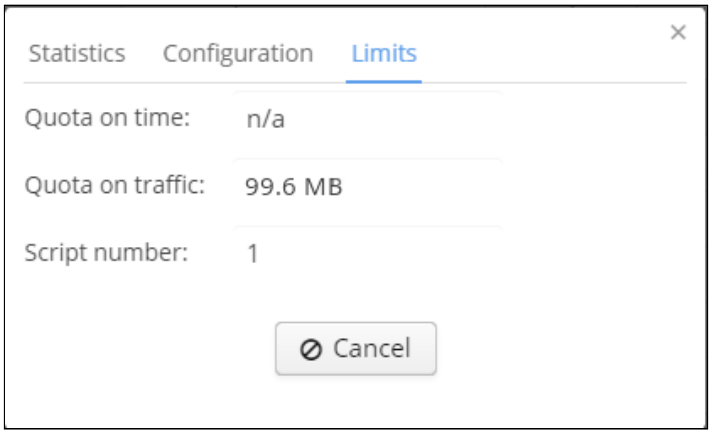
    - Password (obligatory). Field format: length from 4 to 253, only Latin symbols, lowercase and uppercase characters, digits, special symbols: '_', '.', '-', space, '!';
    - Domain or SSID (obligatory);
    - End date;
    - Tariff;
    - Surname;
    - 1st and mid.name;
    - Mobile phone;
    - E-mail;
    - Division;
    - Position;
    - MAC address;
    - Deactivation;
    - Temporary block.

- Registration on the Hotspot portal via access points of other vendors (BRAS). User accounts have the following set of parameters:
    - Login (obligatory). Field format: length from 1 to 50, only Latin symbols, lowercase and uppercase characters, digits, special symbols: '_', '.', '-';
    - Password (obligatory). Field format: length from 4 to 253, only Latin symbols, lowercase and uppercase characters, digits, special symbols: '_', '.', '-', space, '!';
    - Domain (obligatory);
    - End date;
    - Tariff;
    - Surname;
    - 1st and mid.name;
    - Mobile phone;
    - E-mail;
    - Division;
    - Position;
    - MAC address;
    - Deactivation;
    - Temporary block.

"Eltex" AP users and PCRF users have different tariffs, so a user created for authorization via "Eltex" AP will not be able to perform portal authorization via BRAS and vice versa.

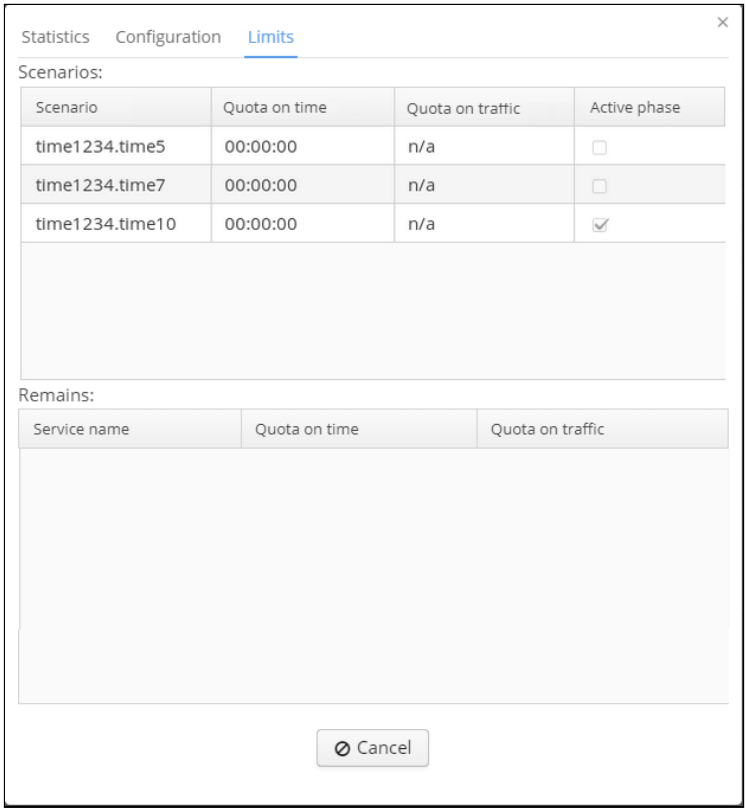
Hotspot users' traffic and time quotas

---



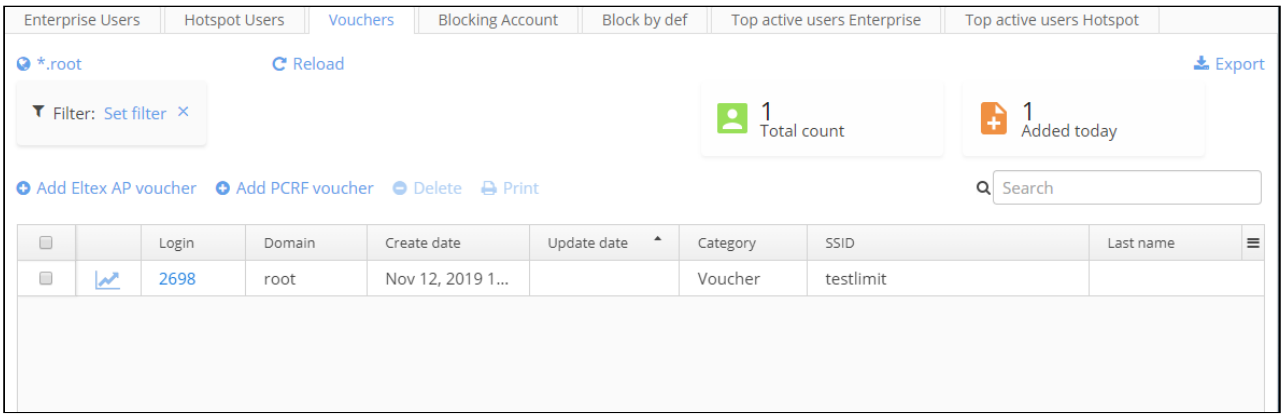

The tab "Limits" contains information on time quota, traffic quota and the number of current scenario.

Time and traffic quota for Hotspot BRAS users




The tab "Limits" for BRAS users contains information on time and traffic quota. The column "Scenario" contains information on a current scenario and a service included into it. Each service added to a scenario is displayed in a separate row. The columns "Time quota" and "Traffic quota" contain information on quotas for each service. "Active phase" — a service that is active.

## Vouchers

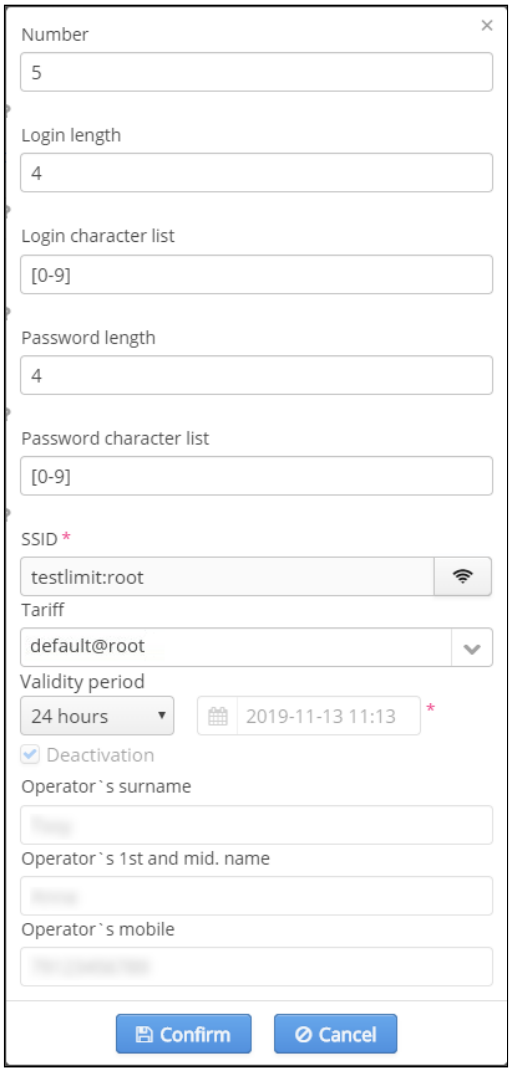



The tab *"Vouchers"* is intended for mass creation of user accounts. There is an opportunity to generate a specified number of user accounts with random logins and passwords and to assign them to users.

This option can be used in organisations where a temporary access to a service is required, for example, in hotels.

Hotel staff should put information on receiving a voucher by a guest to other hotel management systems (full names and passport data of clients/guests are stored in business process management programs). Beginning with the version 1.8, each "Voucher" entry has additional fields. This fields can be filled in with full name, mobile phone, e-mail and passport data of a client. Wi-Fi B2B Admin Panel stores data on an account under which a user who created or edited an entry entered the system.

### Adding a pool of entries



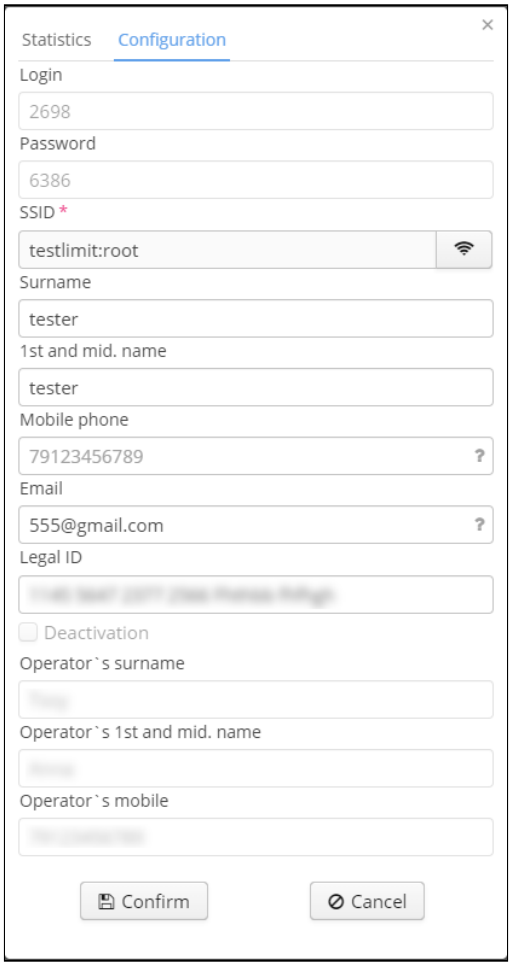

To create a pool of entries, click *"Add"*. A program will display a dialog window where some parameters should be set. These parameters are:

- number;
- password length;
- Domain and SSID;
- tariff;
- validity period.

Set the parameters and click *"Confirm"*. The number of created user accounts will be equal to one specified in the field *"Number"*. Logins and passwords contain only digits and Latin symbols. Password length is specified in the window. All accounts will be created in a specified domain (obligatory parameter) and with specified parameters. Validity period — date and time after which it will be impossible to connect to the network.

If the option **"Auto activating voucher after creation"** is not enabled in the Admin Panel settings, all created vouchers are initially blocked. A voucher can be activated by the Admin Panel administrator.

Enabling vouchers



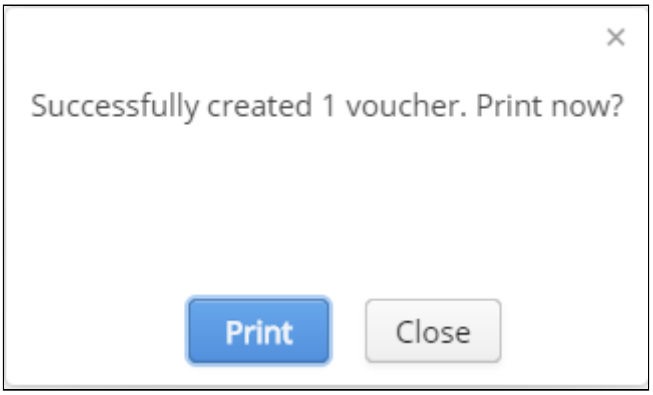

All created entries will be initially blocked. To unblock an entry, enter a full name, mobile phone and passport data of a user. If an option "**Auto activating voucher after creation**" is enabled, all vouchers (options after activating) will be enabled automatically after their creation, but if only one of obligatory fields is filled in, a voucher will be blocked. To fill in the remaining fields:

- Surname;
- 1st and mid.name;
- Mobile phone;
- Email;
- Passport data;

click on the login. A window with optional fields will be opened.

Accounts of "Voucher" type can be created only for an open network with portal authorization (except for a scheme with BRAS).

### Printing vouchers




| | |
|---|---|
| Domain: root<br>Login: 4620<br>Password: 5678<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 8800<br>Password: 8752<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 6807<br>Password: 9521<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 5256<br>Password: 4030<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 2281<br>Password: 3508<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 3743<br>Password: 2603<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 0048<br>Password: 3179<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 7633<br>Password: 1004<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 2744<br>Password: 3597<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 5264<br>Password: 8768<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 2605<br>Password: 8927<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 3337<br>Password: 5080<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 2642<br>Password: 1329<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 4362<br>Password: 9510<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 2252<br>Password: 1029<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 4171<br>Password: 3256<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 4736<br>Password: 7096<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 1995<br>Password: 1781<br>Valid till: 2019-11-14 09:32 |
| Domain: root<br>Login: 4427<br>Password: 1788<br>Valid till: 2019-11-14 09:32 | Domain: root<br>Login: 0206<br>Password: 2273<br>Valid till: 2019-11-14 09:32 |

To print created vouchers, select corresponding rows in the table and click *"Print"*. The program will generate a .pdf file ready for print and show its preview in a modal window. If a printer is set up in a user's operating system, vouchers can be directly printed.

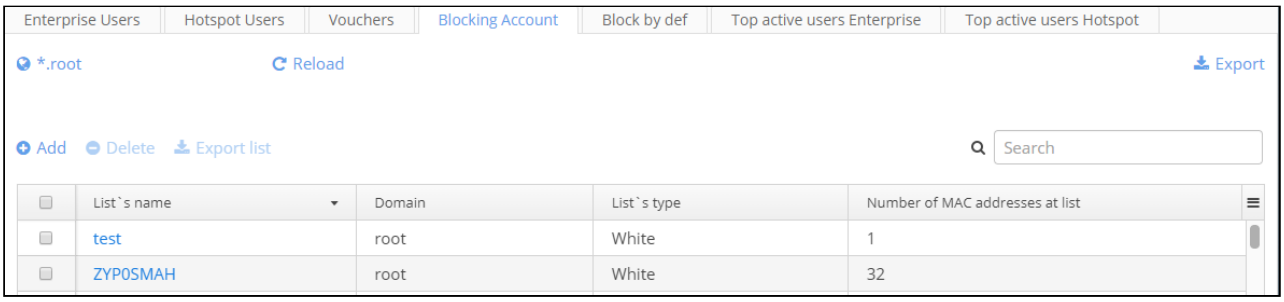
Data for logging into a network (vouchers) are printed 20 per one A4 sheet with portrait orientation and lines used. It allows printing a large number of vouchers in the convenient format in order to give them to guests at check in.

### Deleting a pool

Overdue entries deleting is performed manually by selecting required entries and clicking the button *"Delete"*. If an operator deletes a currently used voucher, connection will not be lost.

A user will not be able to pass authorization again after closing a connection.

## Blocking Account




This tab is intended for MAC address lists creation. Such lists are used to restrict access to the Hotspot portal. There are two types of lists:

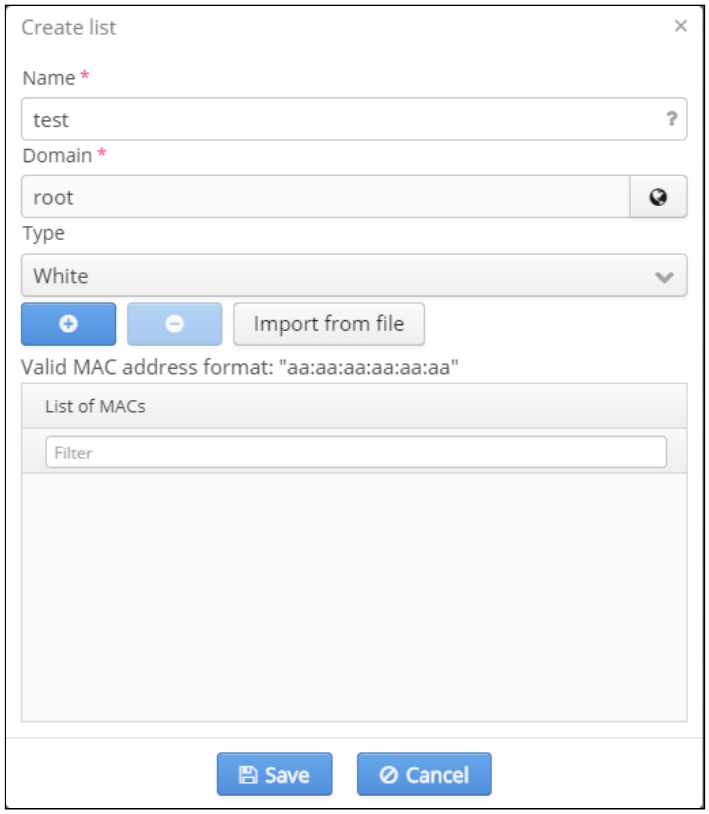
- White lists — all addresses contained in them have access to the portal while others do not;
- Black lists — all addresses have access to the portal while addresses included into a list do not.

To enable filtering by MAC address on the Hotspot portal, create a list and link it to the portal via the Portal Constructor.

### Filtering lists

Entries can be filtered by domain, name or type. To find a list in which a certain MAC address is contained, enter this address in the following format: "11:22:33:aa:bb:cc".

### Adding a list

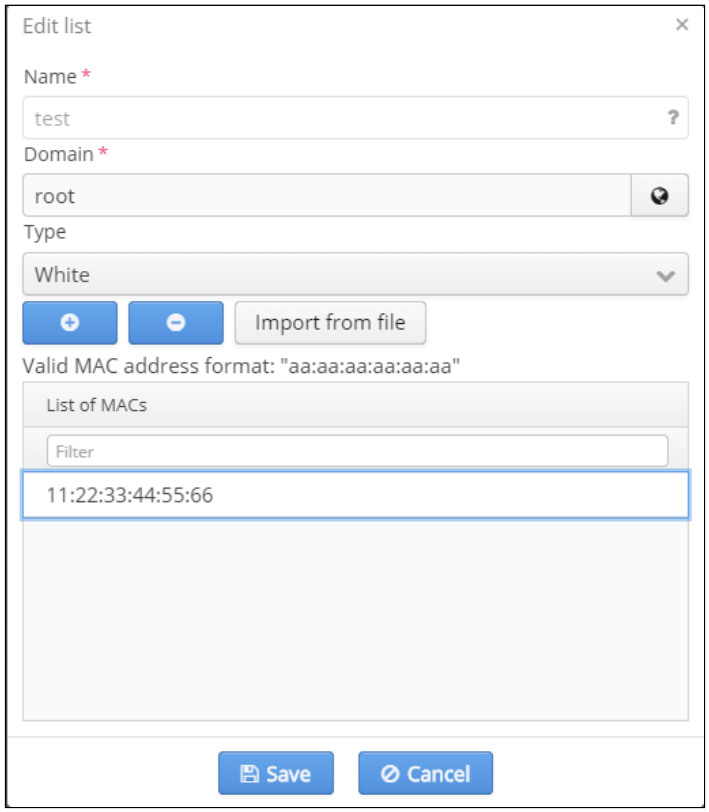



After clicking the button *"Add"* a modal window for adding a MAC address list will appear. A defined set of parameters can be configured in special fields. Fields marked with "*" are obligatory. An attempt to save an entry with empty or incorrectly filled obligatory fields will be rejected. Empty or incorrectly filled fields are highlighted in red. When a mouse is moved over a field, a tip with rules on completing this field is displayed.

The following control elements are available:

- *"+"* — add a new entry to the table;
- *"-"* — delete a selected entry from the table;
- *Import from file* — import a list from a text file.
- Search bar — search for a MAC address in the list.

Viewing and editing a list

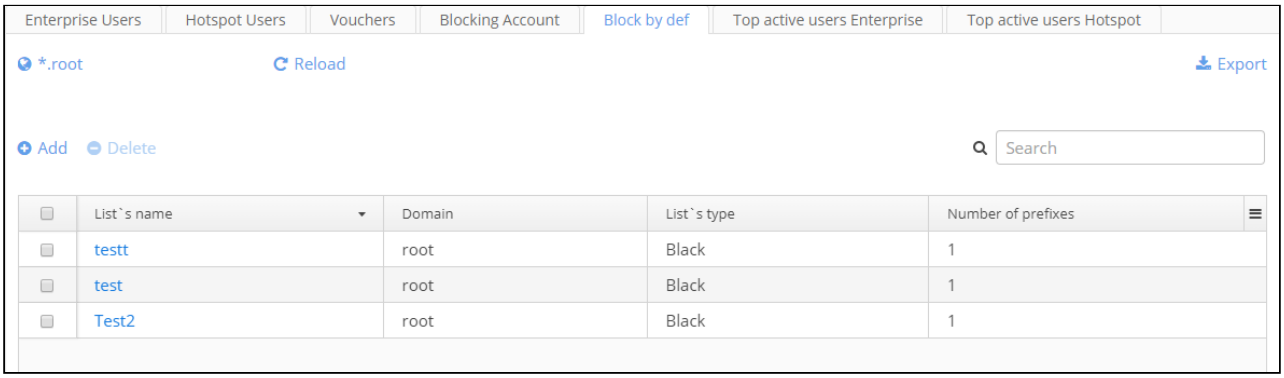



To view and edit a MAC address list, click on its name. A modal window for list editing will be opened.

Deleting a list

To delete a list, set a checkbox in a corresponding row and click the button "-".

Block by def



The tab "Block by def" is used for creating black and white lists containing number prefixes (DEF) or full numbers. These lists are used to restrict access to the Hotspot portal. Blocking by phone number is similar to blocking by MAC address, but subscribers' phone numbers are specified instead of MAC. There are two types of lists:

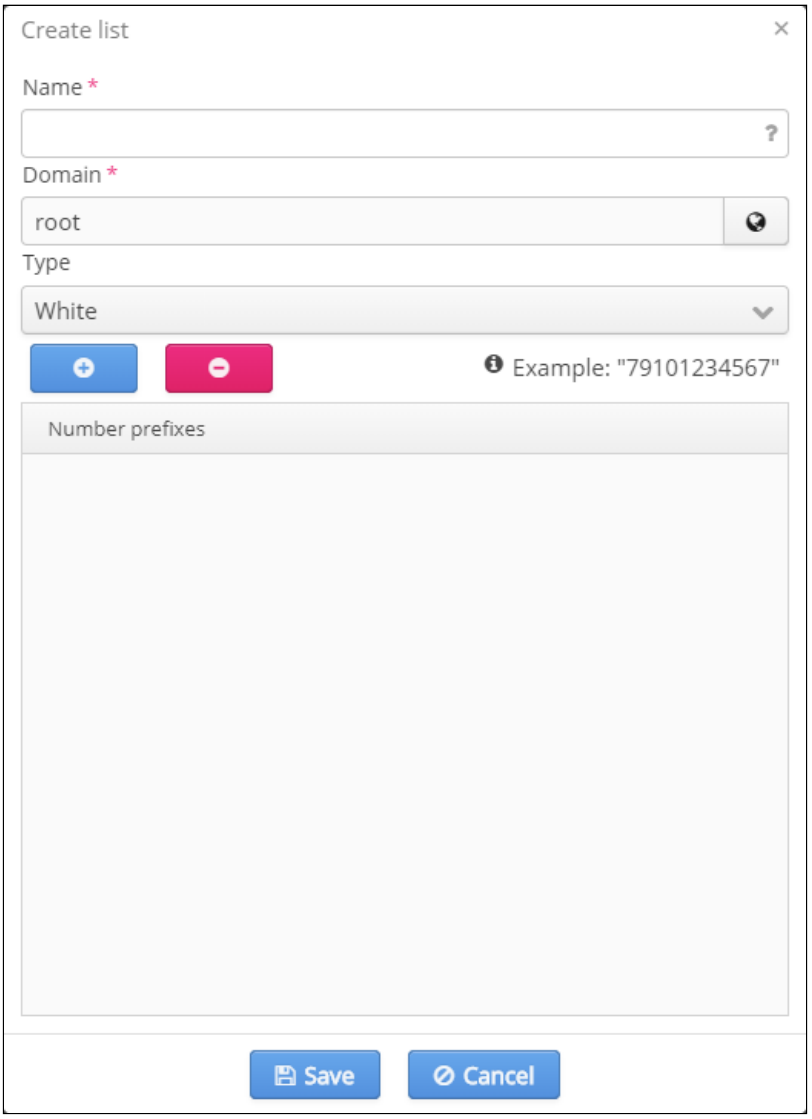
- White lists — all addresses contained in them have access to the portal while others do not;
- Black lists — all addresses have access to the portal while addresses included into a list do not.

**How does it work**

- Assume it is necessary to block users whose phone numbers start with 7654. Then create a list, enter a number part 7654, select the type "black" and link the list to the portal. Now all users whose number starts with 7654 will not be able to enter the system.
- If one number or several different numbers should be blocked: create a list, select the type "black", enter a whole number (example: 76543562293). If necessary, add a few more numbers by clicking the icon  , save the results. Only a user whose phone number is 76543562293 will not be able to pass authorization on the Hotspot portal.
- The last way is creating a white list. To do this, create a new list, select the type "white" and enter a number prefix or a whole number. Now only subscribers having phone numbers from the white list will be able to access the Hotspot portal.

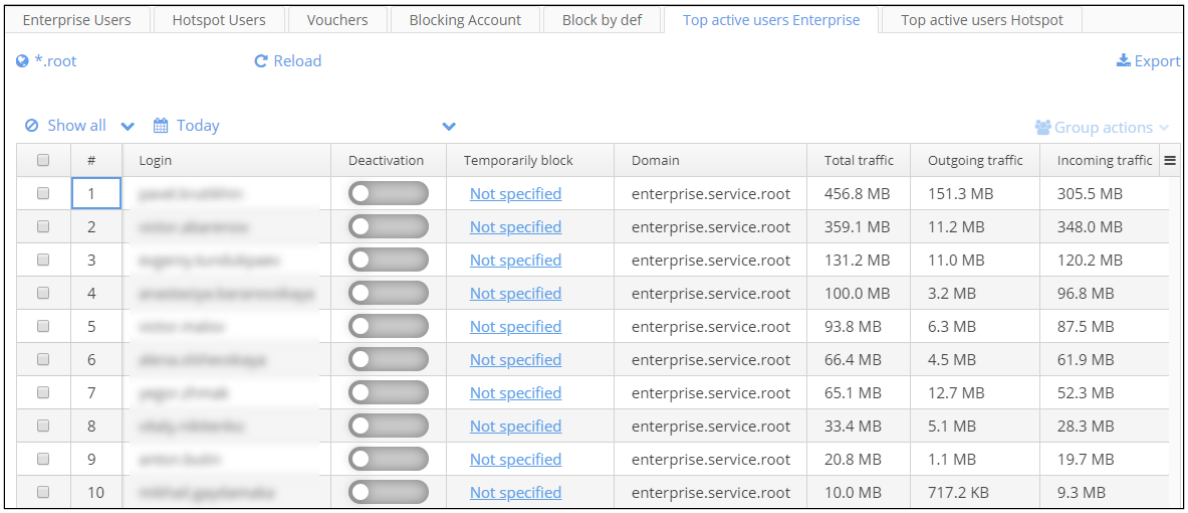
Списки можно отфильтровать как по домену так и по имени.

Creating a list



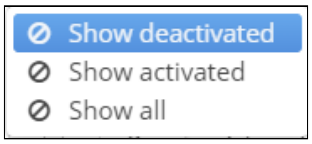

- Name — a unique name of a list;
- Domain — a domain to which a list will belong;
- Type — a pull-down menu where a list type is selected;
- The icon  — when the icon is clicked, an empty row to which a number or its part should be entered appears in the table.
- The icon  — when the icon is clicked, a selected row can be deleted.

Top active users Enterprise



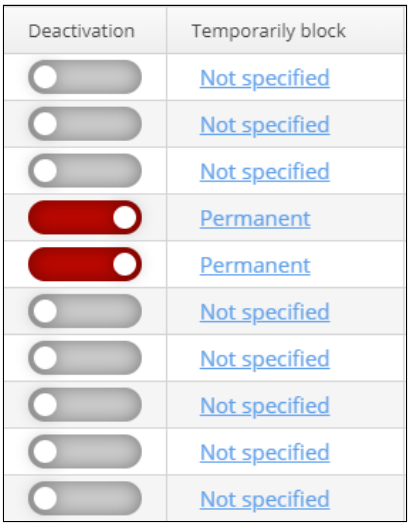

| # | Login | Deactivation | Temporarily block | Domain | Total traffic | Outgoing traffic | Incoming traffic |
|---|---|---|---|---|---|---|---|
| 1 | [redacted] | | Not specified | enterprise.service.root | 456.8 MB | 151.3 MB | 305.5 MB |
| 2 | [redacted] | | Not specified | enterprise.service.root | 359.1 MB | 11.2 MB | 348.0 MB |
| 3 | [redacted] | | Not specified | enterprise.service.root | 131.2 MB | 11.0 MB | 120.2 MB |
| 4 | [redacted] | | Not specified | enterprise.service.root | 100.0 MB | 3.2 MB | 96.8 MB |
| 5 | [redacted] | | Not specified | enterprise.service.root | 93.8 MB | 6.3 MB | 87.5 MB |
| 6 | [redacted] | | Not specified | enterprise.service.root | 66.4 MB | 4.5 MB | 61.9 MB |
| 7 | [redacted] | | Not specified | enterprise.service.root | 65.1 MB | 12.7 MB | 52.3 MB |
| 8 | [redacted] | | Not specified | enterprise.service.root | 33.4 MB | 5.1 MB | 28.3 MB |
| 9 | [redacted] | | Not specified | enterprise.service.root | 20.8 MB | 1.1 MB | 19.7 MB |
| 10 | [redacted] | | Not specified | enterprise.service.root | 10.0 MB | 717.2 KB | 9.3 MB |

The table "Top active users Enterprise" contains information on enterprise users with the highest traffic consumption and is required to block and unblock users temporarily or permanently.
By default, users with higher total traffic are displayed first in the table. There is an opportunity to filter users by Total, Outgoing or Incoming traffic.



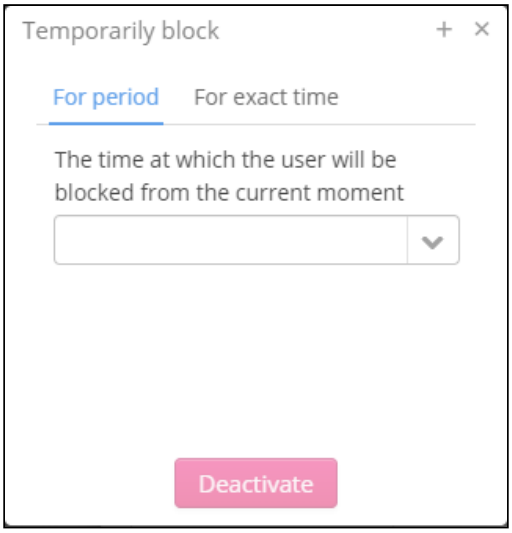

Suggested filters allow displaying activated, deactivated or all users. Filtering is enabled via clicking a corresponding icon.

## Blocking operations



| Deactivation | Temporarily block |
|---|---|
| | Not specified |
| | Not specified |
| | Not specified |
| | Permanent |
| | Permanent |
| | Not specified |
| | Not specified |
| | Not specified |
| | Not specified |
| | Not specified |

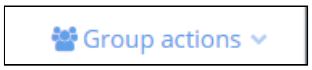
To block a user permanently, click the icon . The blocking state indicator will change its colour from grey to red , and a user will be blocked. To block a user temporarily, click the icon Not specified in the column "Temporarily block". The window "Temporarily block" will be opened.




Two tabs are available in the window: The tab "For period" where the time period during which a user will be blocked may be set only to 1 hour, 2 hours, 6 hours or 1 day. The tab "For exact time" where any time period may be flexibly set.

For example, to block a user for 2 days, open the section "Temporarily block", select the tab "Exact time" and click the icon . In the opened calendar, select date and time for a user to be unblocked. Click Deactivate . A user is successfully blocked. Unblocking date and time are specified in the column "Temporarily block".

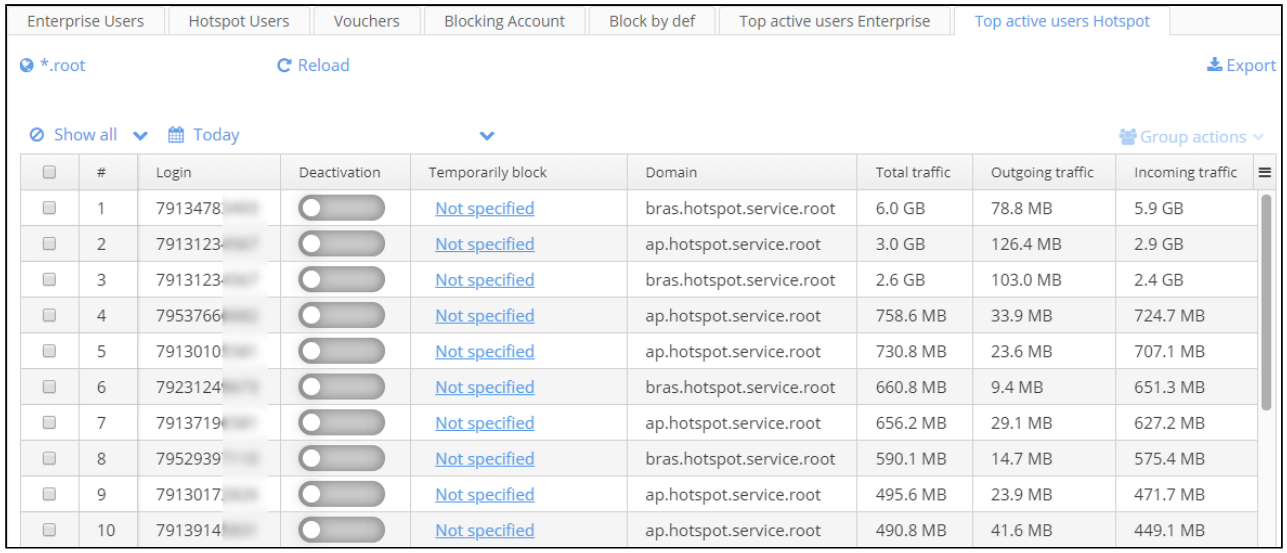
Group actions for blocking




To block several users at the same time, group operations are available. When less than two users are selected, the widget "Group actions" cannot be clicked. When two or more users are selected, the widget "Group activities" becomes available. When the icon Group actions is clicked, a drop-down list will be opened with the following operations available: Deactivate selected, Activate selected and Deactivate temporarily. Operations for blocking a group of users are similar to operations for blocking one user.

To quickly select several users, left-click the checkbox opposite the first user and move your mouse down to the required entry. Release the mouse button.

Top active users Hotspot




The table "Top active users Hotspot" contains information on Hotspot users with high traffic consumption. A type of blocking is specified here (temporary or permanent). A phone number used for authorization, a user account created via the Admin Panel (or in other ways) will be displayed in the column "Login". Each entry contains blocking state (is a user blocked or not) and blocking time (if a user is blocked temporarily). Total, Outgoing and Incoming traffic.

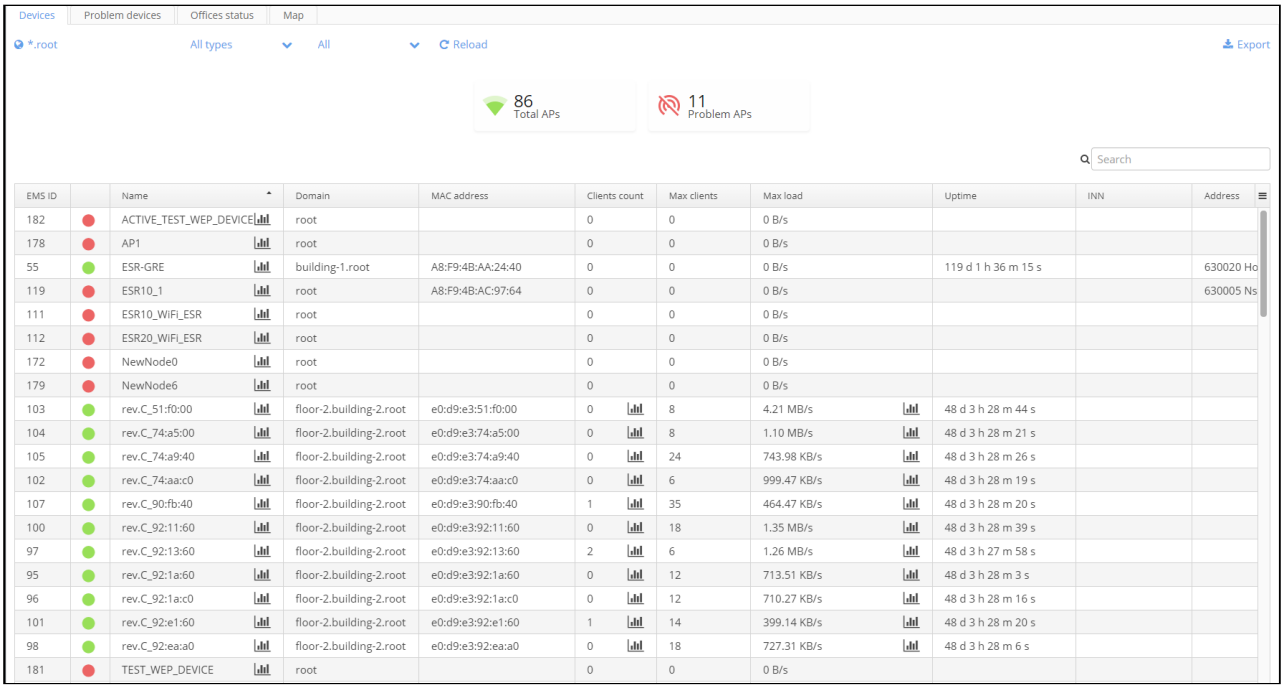
Blocking and unblocking operations are similar to ones in the tab "Top active users Enterprise".

By default, users with higher total traffic are displayed first in the table. There is an opportunity to filter users by Total, Outgoing or Incoming traffic.

## Access points

The section is intended for viewing basic data on device operation (access points and client esr-10).

Devices




| EMS ID | | Name | Domain | MAC address | Clients count | Max clients | Max load | Uptime | INN | Address |
|---|---|---|---|---|---|---|---|---|---|---|
| 182 | | ACTIVE_TEST_WEP_DEVICE | root | | 0 | 0 | 0 B/s | | | |
| 178 | | AP1 | root | | 0 | 0 | 0 B/s | | | |
| 55 | | ESR-GRE | building-1.root | A8:F9:4B:AA:24:40 | 0 | 0 | 0 B/s | 119 d 1 h 36 m 15 s | | 630020 Ho |
| 119 | | ESR10_1 | root | A8:F9:4B:AC:97:64 | 0 | 0 | 0 B/s | | | 630005 Ns |
| 111 | | ESR10_WiFi_ESR | root | | 0 | 0 | 0 B/s | | | |
| 112 | | ESR20_WiFi_ESR | root | | 0 | 0 | 0 B/s | | | |
| 172 | | NewNode0 | root | | 0 | 0 | 0 B/s | | | |
| 179 | | NewNode6 | root | | 0 | 0 | 0 B/s | | | |
| 103 | | rev.C_51:f0:00 | floor-2.building-2.root | e0:d9:e3:51:f0:00 | 0 | 8 | 4.21 MB/s | 48 d 3 h 28 m 44 s | | |
| 104 | | rev.C_74:a5:00 | floor-2.building-2.root | e0:d9:e3:74:a5:00 | 0 | 8 | 1.10 MB/s | 48 d 3 h 28 m 21 s | | |
| 105 | | rev.C_74:a9:40 | floor-2.building-2.root | e0:d9:e3:74:a9:40 | 0 | 24 | 743.98 KB/s | 48 d 3 h 28 m 26 s | | |
| 102 | | rev.C_74:aa:c0 | floor-2.building-2.root | e0:d9:e3:74:aa:c0 | 0 | 6 | 999.47 KB/s | 48 d 3 h 28 m 19 s | | |
| 107 | | rev.C_90:fb:40 | floor-2.building-2.root | e0:d9:e3:90:fb:40 | 1 | 35 | 464.47 KB/s | 48 d 3 h 28 m 20 s | | |
| 100 | | rev.C_92:11:60 | floor-2.building-2.root | e0:d9:e3:92:11:60 | 0 | 18 | 1.35 MB/s | 48 d 3 h 28 m 39 s | | |
| 97 | | rev.C_92:13:60 | floor-2.building-2.root | e0:d9:e3:92:13:60 | 2 | 6 | 1.26 MB/s | 48 d 3 h 27 m 58 s | | |
| 95 | | rev.C_92:1a:60 | floor-2.building-2.root | e0:d9:e3:92:1a:60 | 0 | 12 | 713.51 KB/s | 48 d 3 h 28 m 3 s | | |
| 96 | | rev.C_92:1a:c0 | floor-2.building-2.root | e0:d9:e3:92:1a:c0 | 0 | 12 | 710.27 KB/s | 48 d 3 h 28 m 16 s | | |
| 101 | | rev.C_92:e1:60 | floor-2.building-2.root | e0:d9:e3:92:e1:60 | 1 | 14 | 399.14 KB/s | 48 d 3 h 28 m 20 s | | |
| 98 | | rev.C_92:ea:a0 | floor-2.building-2.root | e0:d9:e3:92:ea:a0 | 0 | 18 | 727.31 KB/s | 48 d 3 h 28 m 6 s | | |
| 181 | | TEST_WEP_DEVICE | root | | 0 | 0 | 0 B/s | | | |

The tab "Devices" contains a table with information on devices:

- EMS_ID — an access point's number in the management system;
- Access point state — a color state indicator:
  - green — access point is all right;
  - yellow — access point is operating, but an error has occurred on it;
  - red — an access point is unreachable from the management system;
  - grey — an access point is taken out of service (not pinged).
- Name — access point name in the management system;
- Domain;
- MAC address — access point MAC address;
- Clients count — the number of clients connected to an AP;
- Uptime — access point operating time;
- Address — device address;
- Max load — maximum traffic load of a network interface.

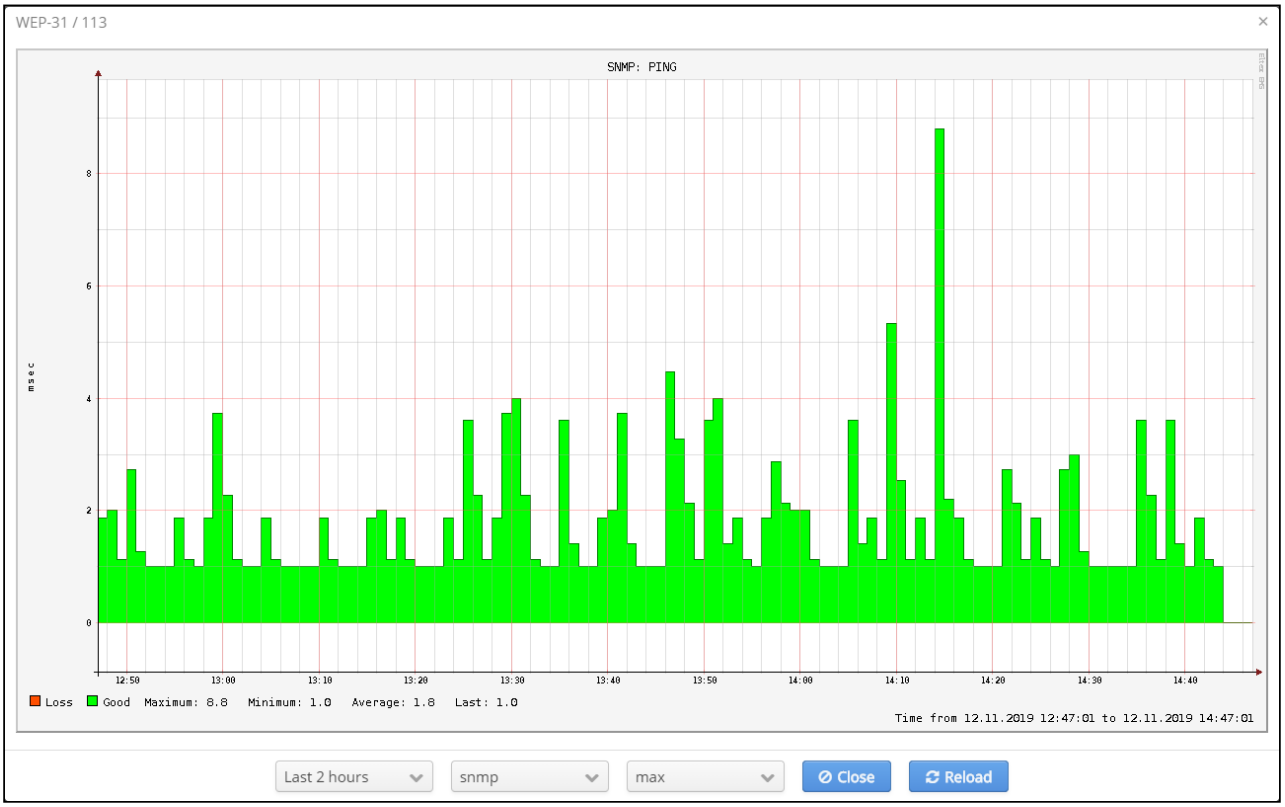
When any cell of the column "Max load" is clicked, a window with a chart showing an AP network interface load will be opened.
The two counters are located above the table. The first counter indicates the total number of access points, and the second one — the number of inaccessible access points (marked as problem APs).

To perform filtering by the domain, specify it in the upper left corner.
To perform filtering by the device type, specify it in the upper left corner.
To perform filtering by OTT attribute, specify OTT it in the upper left corner:

- ALL — all devices;
- Not OTT — all devices without OTT configured;
- OTT Connected (Client) — client devices with OTT configured;

- OTT ServiceProvider — devices to which client OTT devices establish IPSec tunnels;

To perform a search by MAC address, location (address) or name, the field "Search" can be used.
To export data in .csv format, click the button "Export".

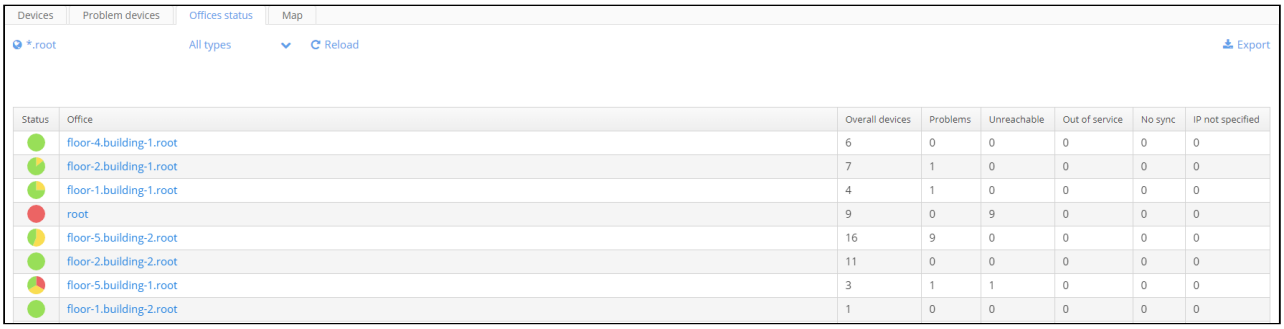



When an access point's name is clicked, a window with a device reachability test chart will be displayed. Time period for which data will be displayed, ping type (SNMP/ICMP) and data aggregation type (min/max) can be selected in the window.
To display all cases of losing connection to a device, select the "min" aggregation type.

### Problem devices

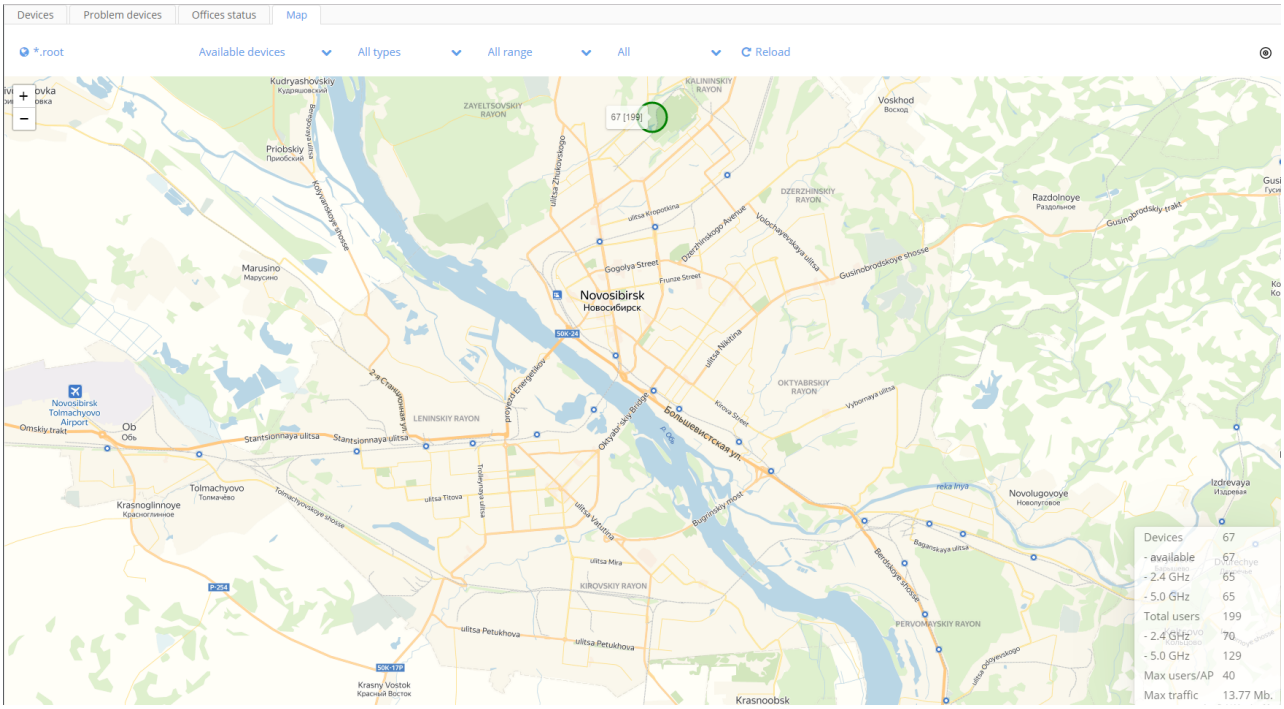
The table located on the tab "Problem devices" is similar to one located on the previous tab, but only devices in "Unreachable" state are displayed in it. A filter by the domain is also located on the page.

### Offices status




On this tab, information on devices grouped into domains is displayed. For each group of devices, information is displayed in the form of a pie chart showing operating and problem devices (the column "Status"). Other columns contain information on the number of problem, unreachable devices and devices out of service. The filter by the domain is also located on the tab.

## Map




Devices are displayed on the map according to locations specified in each device's configuration.
Filters:

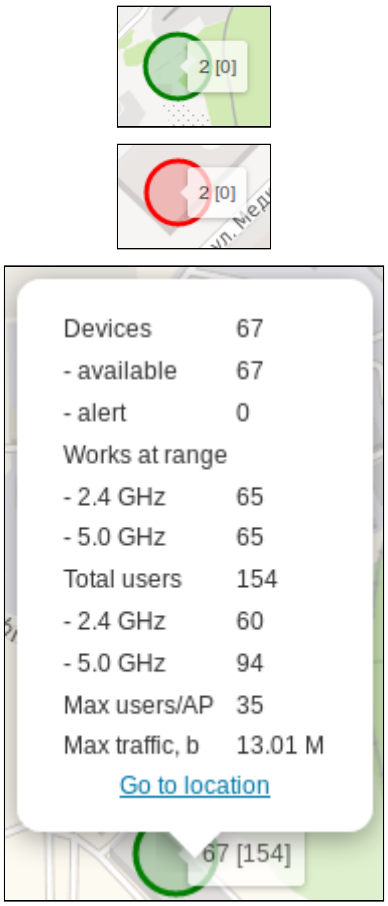
- by domains
- by device availability (availability is defined by results of ICMP and SNMP pings in EMS. A device is considered as unavailable if both pings were lost).
- by device type

- by frequency range (if "All range" is selected, all access points are displayed. If a certain range (2.4GHz or 5GHz) is selected, only those access points that have a SSID in this range will be displayed).

After changing a filter, click "Reload" to apply the changes.

The button is used for moving to a user's location.

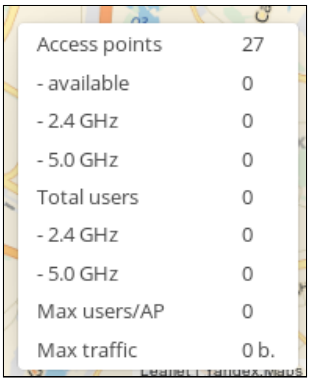
> ⚠ Geolocation is available only when HTTPS is used. If the Admin Panel is accessed via HTTP, geolocation will be disabled due to browsers' security policies. To successfully define where an AP is located, grant geolocation rights to a browser.




Functioning access points are displayed as green circles. Access points, access to which has been lost are red circles. Access points having the same address are grouped together. Next to a group of access points consolidated information is displayed (the number of access points in a group and the number of connected users in square brackets). If there is at least one unavailable access point, a group will be highlighted red.

When you zoom in, the closest access points are grouped together. A subtle displacement of AP groups displayed near screen edges is possible.

When an object is selected, information on the number of devices and clients is displayed for this object. Follow the link "Go to location" to open a list of devices connected to the object.




In the lower part of the screen consolidated information is displayed:

- Devices available — the number of displayed access points (considering filters and coordinates of the selected area)
- Devices 2.4GHz, 5.0GHz — the number of corresponding SSIDs
- Total users 2.4GHz, 5.0GHz — the number of users in the ranges
- Max users/AP — the maximum number of users connected to one access point
- Max traffic — the maximum volume of current traffic

## Event log

The section *"Event log"* contains two tabs: *"Event log" and "Wi-Fi users Event log".*

All changes made by system operators are added to event logs. List of operations:

- creating entries;
- deleting entries;
- updating entries;
- starting/reloading.

System-wide information is also stored in the event logs.

Entries contain the following fields:

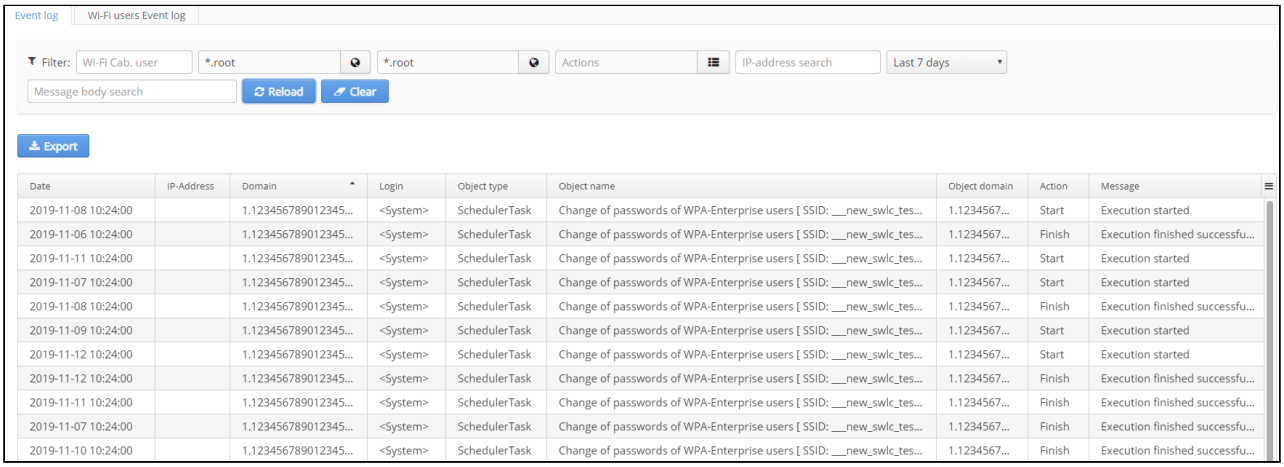
- date and time of an event (server time);
- IP address of a host from which an operation was performed (if available);
- login and domain of a user performing an operation (if available);
- name of an object modified;
- action code: Launch, Create, Delete, Edit;
- interpretive message.

To view details on any entry of event logs, left-click on it. A modal dialog with full information will be opened. To close a dialog, click *"OK"*.

The button *"Export"* allows exporting entries displayed on the screen (selected by a current filter) as a text file to a user's PC.

Access to event viewing depends on a user's role and domain.

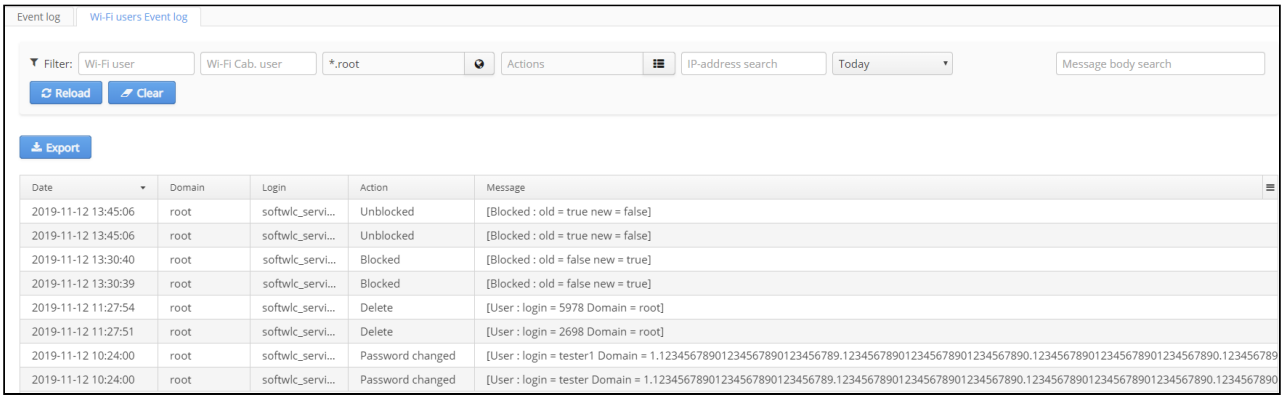
## Event log




The tab *"Event log"* is used to display a log of system events and a log of system parameters changes.The following events are stored in the log:

- updating Wi-Fi B2B Admin Panel system settings;
- updating Admin Panel system roles;
- updating Admin Panel system users (operators);
- updating domains;
- updating firmware;
- stopping, starting and restarting a server.

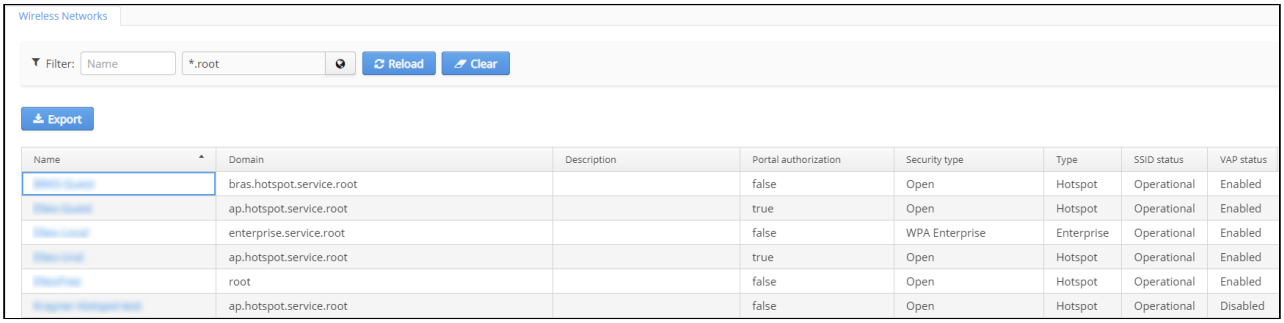
## Wi-Fi users event log




The tab *"Wi-Fi users event log"* is used to display a full change log for Wi-Fi user accounts. The tab allows viewing all actions on accounts, from creating an account to deleting it.

The column *"Message"* is used for the system to store names and contents of updated fields. Passwords given to users are replaced with * in logs.

## Wireless networks



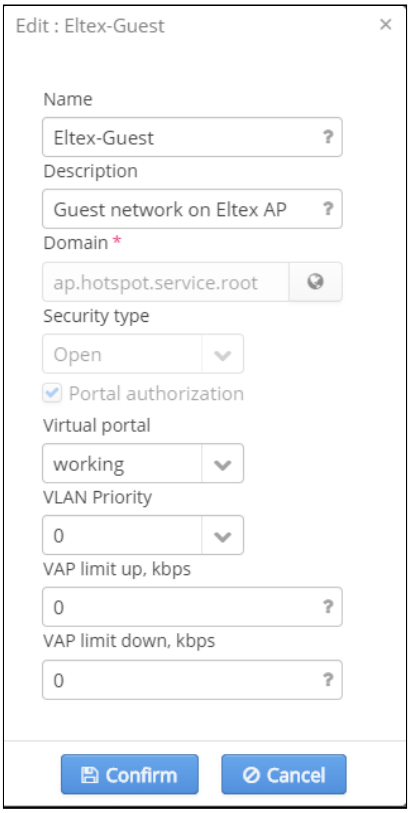

The section "Wireless networks" contains general information on main SSID parameters user in the system and their state. The table on the tab "Wireless networks" contains information:

- SSID name
- SSID domain
- SSID description
- Portal authorization status
- Security type
- SSID status

The filter by domain is available on the tab.

Editing wireless networks

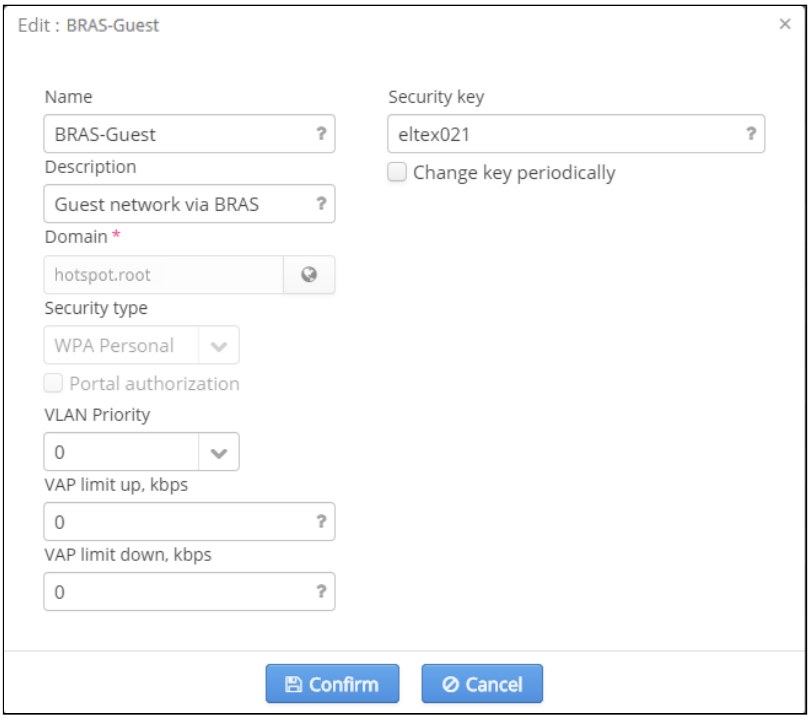
Editing networks with portal authorization




In networks with WPA-personal authorization, there is an opportunity to configure a WPA key used for authorization in this network and also to create a task for its automatic replacement.
The following parameters can also be edited:

- **Name** — SSID name
- **Description** — a comment for a SSID administrator
- **SSID status** — whether a SSID is operating or not
- **VLAN Priority** — setting a priority mark to a VLAN used for SSID
- **VAP limit up** — uplink speed limit for VAP (common for all connected users)
- **VAP limit down** — downlink speed limit for VAP (common for all connected users)

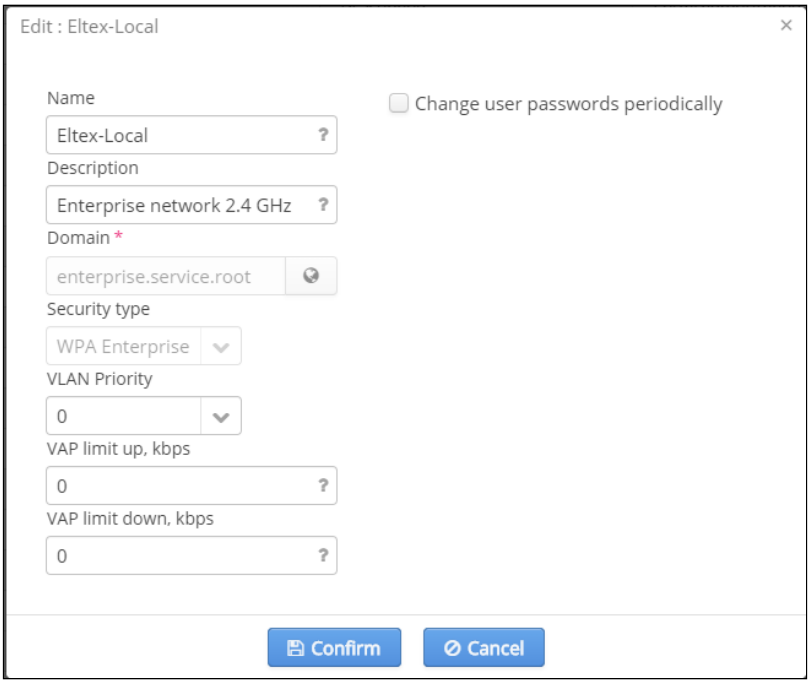
Editing networks with WPA-personal authorization




In networks with WPA-personal authorization, there is an opportunity to configure a WPA key used for authorization in this network and also to create a task for its automatic replacement.
The following parameters can also be edited:

- **Name** — SSID name
- **Description** — a comment for a SSID administrator
- **SSID status** — whether a SSID is operating or not
- **VLAN Priority** — setting a priority mark to a VLAN used for SSID
- **VAP limit up** — uplink speed limit for VAP (common for all connected users)
- **VAP limit down** — downlink speed limit for VAP (common for all connected users)

Editing networks with WPA-enterprise authorization




In networks with WPA-enterprise authorization, an administrator can create a task for automatic change of a certain SSID users' passwords.
The following parameters can also be edited:

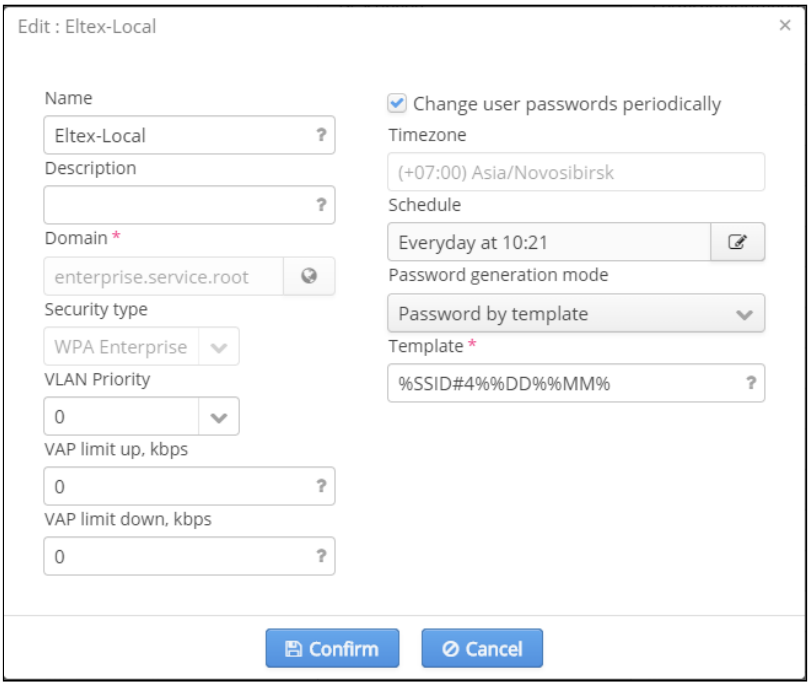
- **Name** — SSID name
- **Description** — a comment for a SSID administrator
- **SSID status** — whether a SSID is operating or not
- **VLAN Priority** — setting a priority mark to a VLAN used for SSID
- **VAP limit up** — uplink speed limit for VAP (common for all connected users)
- **VAP limit down** — downlink speed limit for VAP (common for all connected users)

### Creating tasks for automatic password changing

The Admin Panel allows creating tasks for changing passwords in encrypted networks. The list of created tasks can be seen in the section "Scheduler". Information on task execution is saved in the "Event log".

Mechanisms for password generation are different for different types of authorization, so they will be considered separately.

#### Creating a task for password changing in networks with WPA-enterprise authorization




To create a task for password changing in a network with WPA-enterprise authorization, check the checkbox "Change user passwords periodically" in the window for SSID editing.

As tasks for scheduled password changing are initiated considering a timezone, one for SSID domain is specified in the field "Timezone". The parameter cannot be modified and is displayed for information.

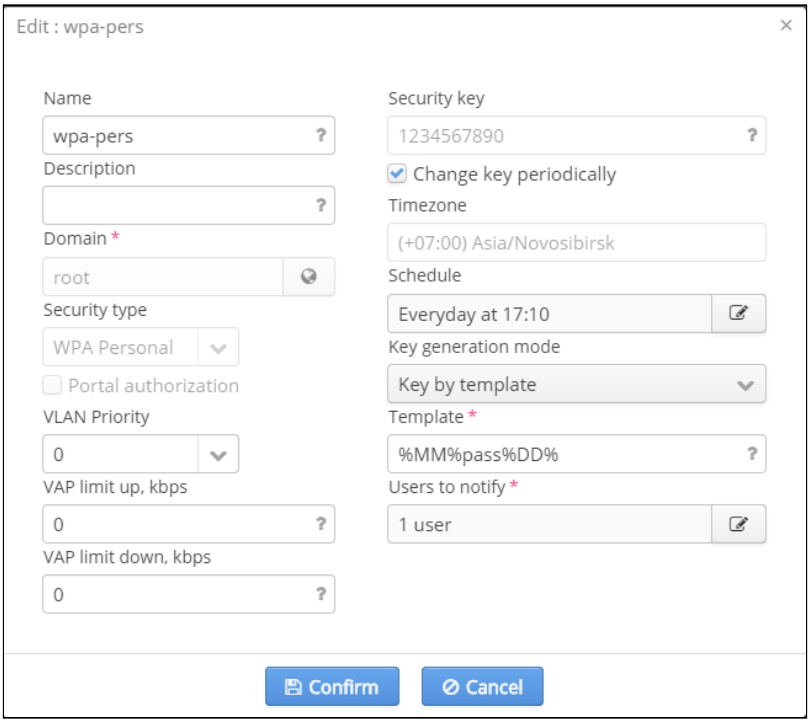
After checking the checkbox, options for task configuration will be displayed in the window. The following parameters should be specified:

- Schedule – a task initiation schedule, launch time is specified according to a SSID domain's timezone
- Password generation mode (Random password or Password by template):
  - If the mode "Random password" is selected, a length of a generated password is specified in the field "Length" (a password will contain digits and Latin symbols)
  - If the mode "Password by template" is selected, a template is specified in the corresponding field. Tagged expressions (for example, %MM%, %DD%) are specified according to a SSID domain's timezone.

New passwords will be sent to SSID Wi-Fi users via e-mail or SMS, so either e-mail address or phone number should be specified in a user's account for him to receive the password. A user's SSID is specified on the tab "Enterprise users". To check if a user belongs to a SSID, see the parameters "Domain" and

"SSID".
A task will be initiated at the specified time according to a SSID domain's timezone. Task initiation time according to a server's timezone can be seen in the section "Schedule".

Creating a task for password changing in networks with WPA-personal authorization




To create a task for password changing in a network with WPA-personal authorization, check the checkbox "Change user passwords periodically" in the window for SSID editing.

As tasks for scheduled password changing are initiated considering a timezone, one for SSID domain is specified in the field "Timezone". The parameter cannot be modified and is displayed for information.

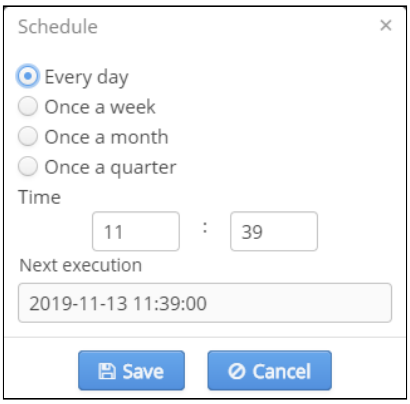
After checking the checkbox, options for task configuration will be displayed in the window. The following parameters should be specified:

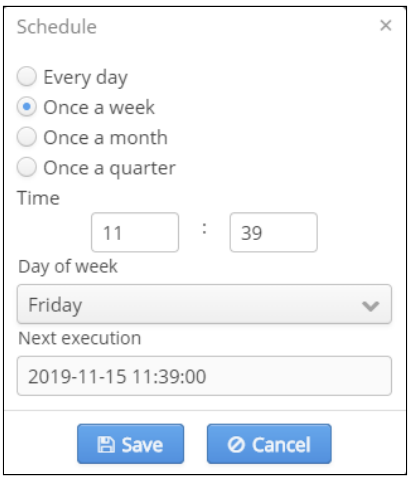
- Schedule – a schedule for task initiation, an interface is similar to one for enterprise authorization. Start time is specified according to a SSID domain's timezone
- Password generation mode (Random password or Password by template):

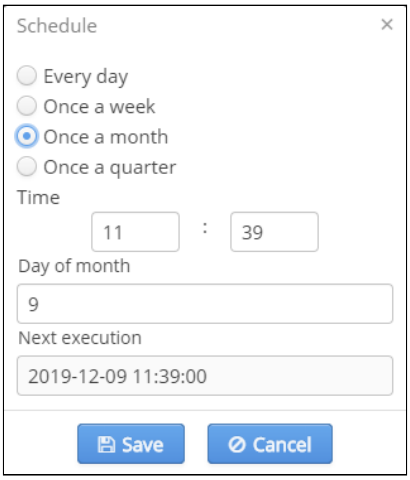
  - If the mode "Random password" is selected, a length of a generated password is specified in the field "Length" (a password will contain digits and Latin symbols)
  - If the mode "Password by template" is selected, a template is specified in the corresponding field. Tagged expressions (for example, %MM%, %DD%) are specified according to a SSID domain's timezone.
- Users to notify – system users to whom notifications on password changes will be sent via e-mail or SMS (e-mail or phone number should be specified in user settings

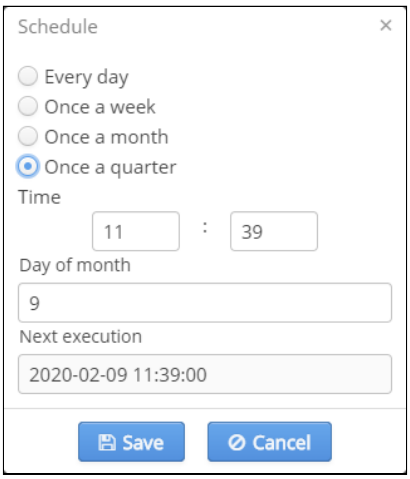
A task will be initiated at the specified time according to a SSID domain's timezone. Task initiation time according to a server's timezone can be seen in the section "Schedule".

### Configuring a schedule





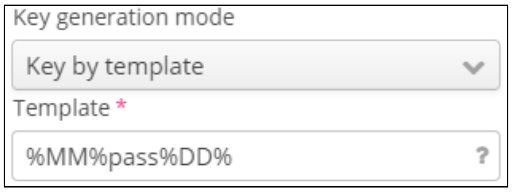

To configure a schedule, select a launch period depending on which the additional parameters will be required:

- Every day — launch time.
- Once a week — day of the week and launch time.
- Once a month — day (date) of the month and launch time.
- Once a quarter — day (date) of the first quarter and launch time.

In the field "Next execution" the date of the next initiation of the task defined according to new settings and SSID domain's timezone will be displayed.

### Configuring templates for key generation

The ability to generate template-based keys is implemented in the password (key) generator. In this case, a key will consist of previously defined elements. Templates are sets of digits, Latin symbols and tags whose values will be defined during password generation:



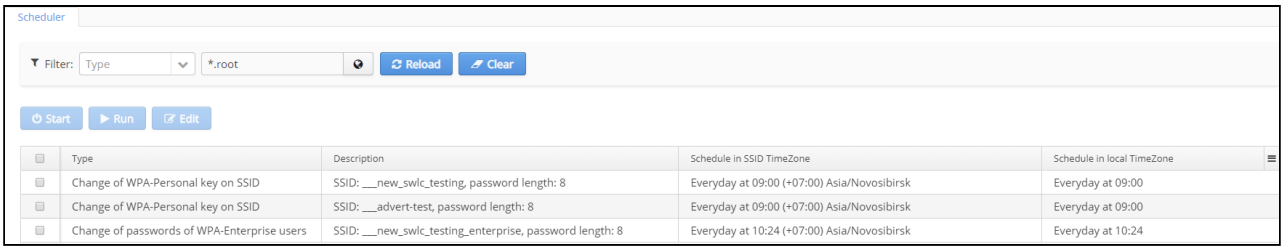

A template should match the following requirements:

- Password length: from 8 to 63 symbols.
- Valid characters: digits, Latin uppercase and lowercase letters, special characters: '-', '_', space and '.'.
- Tagged expressions:
  - %MM% — month number (including leading zeros).
  - %DD% — day number (date) (including leading zeros).
  - %SSID#4% — take last 4 symbols from the SSID name.

The untagged part of a password will not be changed.

Tagged expressions are specified according to the SSID domain's timezone.

## Scheduler




Data on scheduled tasks executed automatically, without user involvement. Information on task initiation and execution is saved to the event log.
Control buttons:

- Start/stop — enable/disable automatic task execution (operations are not deleted).
- Run — run operations manually at the present time.

It is possible to perform actions both on one and on several operations with the same activity status. When operations with different status are selected, the button "Start" becomes inactive. Initiation of tasks being executed is unavailable. If there is an attempt to click the button "Run" during task execution, an error occurs.
Time is displayed according to a timezone of a server specified near the task initiation time.

| Task type | Description |
|---|---|
| Change of WPA-Personal key on SSID | Instruction |
| Notification on license expiration via e-mail | Notifies administrators 90 days prior to license expiration. Also notifies on demo-license usage. |
| Clearing the event log | Deletes old events from the event log upon exceeding 1000000 entries |
| Clearing reports repository | Deletes irrelevant reports |
| Sending notifications on SSID password change | Instruction |

## Reports


The section contains reports commissioned by a user.
Reports are generated as pdf files.
To export a report, click the button "Download".

### Advertising platform

A link to an advertisement provider's website to implement integration.

### Settings

Details on the section "Settings" are given in documentation on the Admin Panel administration.

### PCRF settings

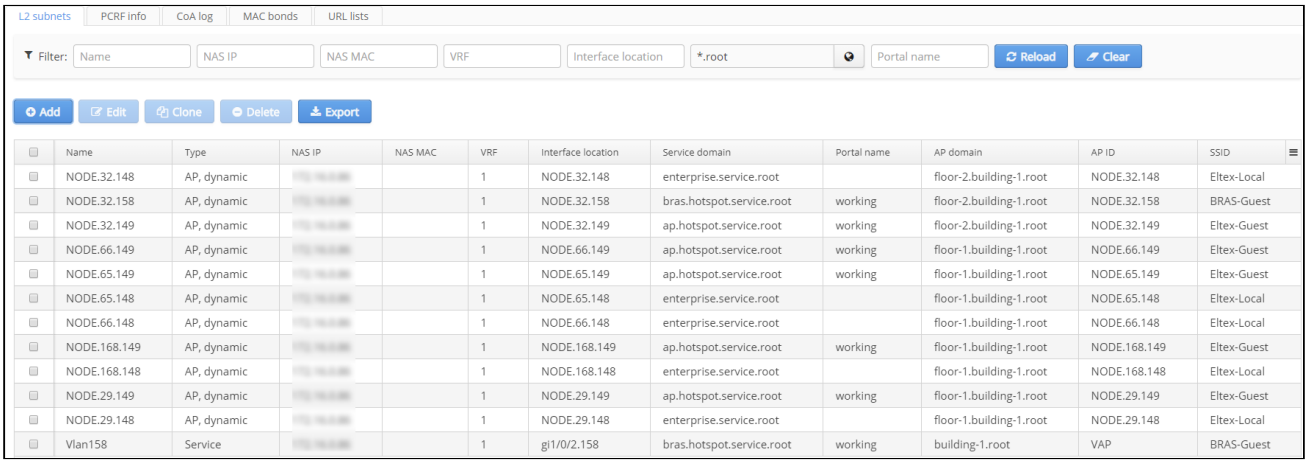
The section *"PCRF settings"* contains basic PCRF settings and allows creating L2 subnetworks, viewing information on the number of BRAS sessions, checking a CoA log and displaying information on stored MAC addresses.

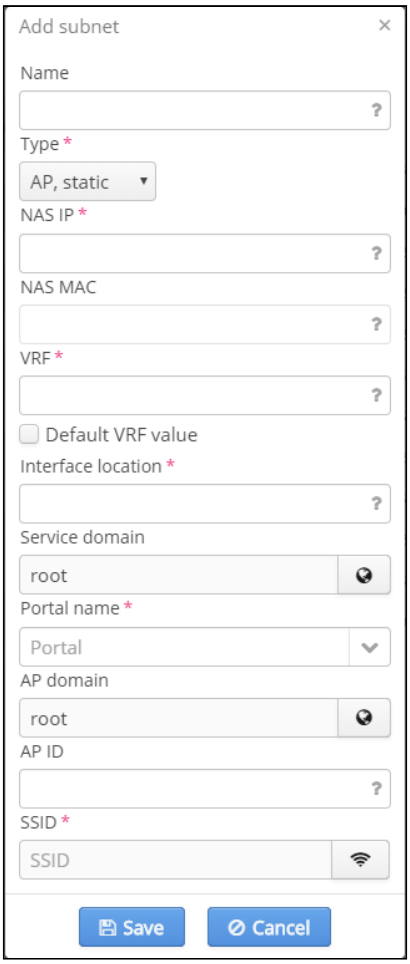
There are 5 tabs in the section:

- *"L2 subnets";*
- *"PCRF info";*
- *"CoA log";*

- *"MAC bonds";*
- *"URL lists".*

## L2 subnets



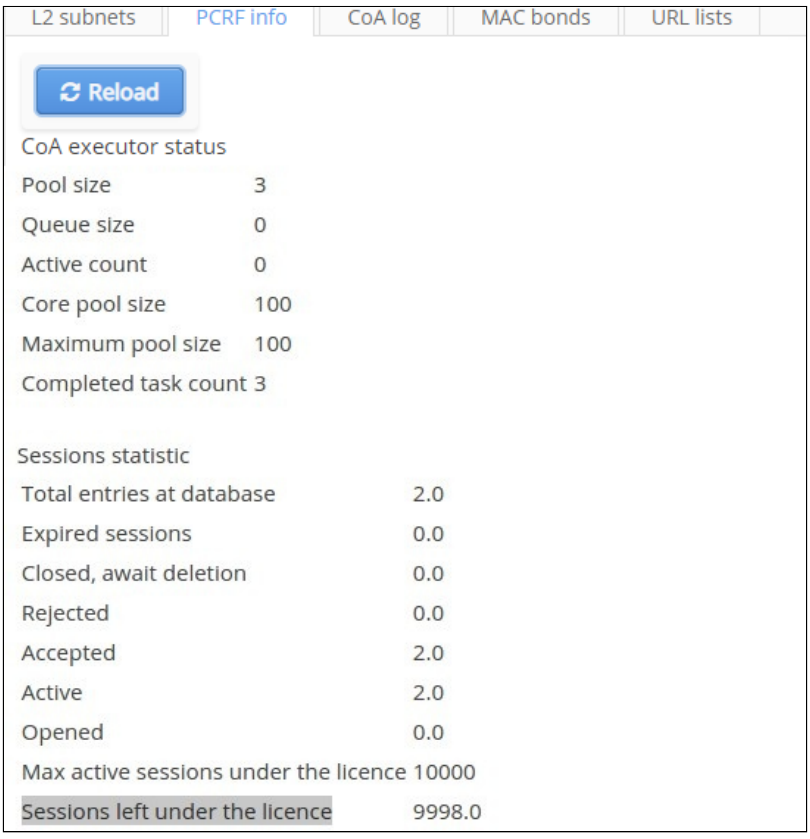
On this tab, L2 subnetworks are created and configured.
There are two types of subnetworks:

- A subnetwork for portal selection
- A subnetwork responsible for statistics, MAC authorization and shapers

Fields for subnetwork configuration:

- *Name — an arbitrary name;*
- *NAS IP* — ESR address, IP address of an interface directed to SoftWLC;
- *VRF* — VRF value;
- *Interface location* — the parameter contains location from ESR interface or L2 interface's name;
- *Name* — portal name in the Portal Constructor;
- *AP domain* — a domain in which and AP is located, i.e. a client's office;
- *AP ID* — an access point's identifier;
- *SSID — SSID name.*

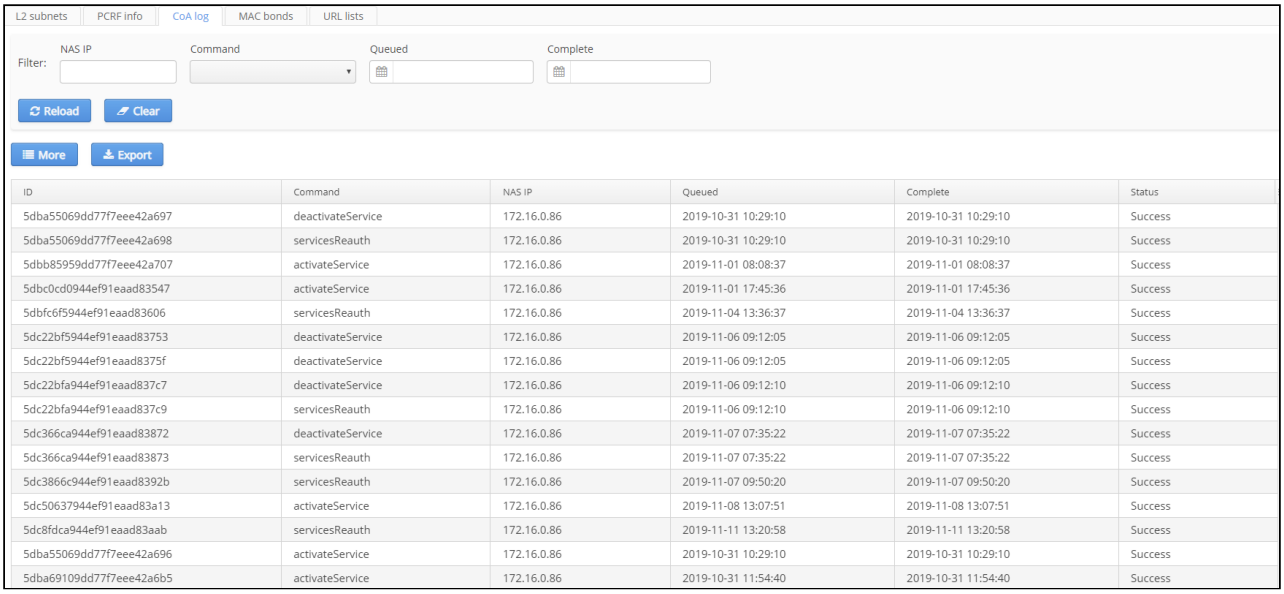
PCRF info



On this tab, information on CoA executor status and statistics on BRAS sessions can be viewed in real time.
BRAS sessions' statuses can be the following:

- Opened — the number of opened sessions without authorization;
- Accepted — the number of accepted sessions;
- *Rejected* — the number of rejected sessions;
- *Closed, await detection* — the number of sessions awaiting termination;
- *Total stored* — the total number of sessions;
- *Active* — the number of authorized sessions;
- *Expired* — the number of expired sessions;
- Max active sessions under the licence — the total number of PCRF licenses;
- Sessions left under the licence — the number of available PCRF licenses.

## CoA log

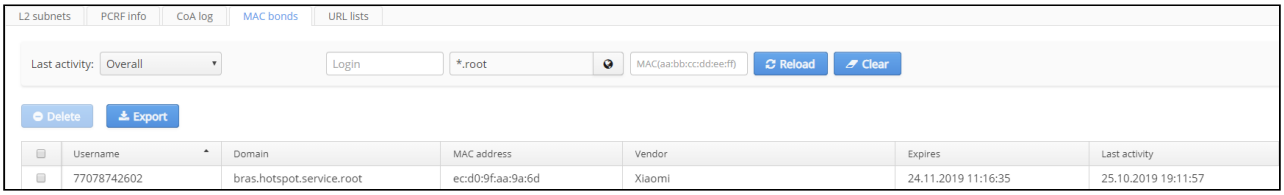



| ID | Command | NAS IP | Queued | Complete | Status |
|---|---|---|---|---|---|
| 5dba55069dd77f7eee42a697 | deactivateService | 172.16.0.86 | 2019-10-31 10:29:10 | 2019-10-31 10:29:10 | Success |
| 5dba55069dd77f7eee42a698 | servicesReauth | 172.16.0.86 | 2019-10-31 10:29:10 | 2019-10-31 10:29:10 | Success |
| 5dbb85959dd77f7eee42a707 | activateService | 172.16.0.86 | 2019-11-01 08:08:37 | 2019-11-01 08:08:37 | Success |
| 5dbc0cd0944ef91eaad83547 | activateService | 172.16.0.86 | 2019-11-01 17:45:36 | 2019-11-01 17:45:36 | Success |
| 5dbfc6f5944ef91eaad83606 | servicesReauth | 172.16.0.86 | 2019-11-04 13:36:37 | 2019-11-04 13:36:37 | Success |
| 5dc22bf5944ef91eaad83753 | deactivateService | 172.16.0.86 | 2019-11-06 09:12:05 | 2019-11-06 09:12:05 | Success |
| 5dc22bf5944ef91eaad8375f | deactivateService | 172.16.0.86 | 2019-11-06 09:12:05 | 2019-11-06 09:12:05 | Success |
| 5dc22bfa944ef91eaad837c7 | deactivateService | 172.16.0.86 | 2019-11-06 09:12:10 | 2019-11-06 09:12:10 | Success |
| 5dc22bfa944ef91eaad837c9 | servicesReauth | 172.16.0.86 | 2019-11-06 09:12:10 | 2019-11-06 09:12:10 | Success |
| 5dc366ca944ef91eaad83872 | deactivateService | 172.16.0.86 | 2019-11-07 07:35:22 | 2019-11-07 07:35:22 | Success |
| 5dc366ca944ef91eaad83873 | servicesReauth | 172.16.0.86 | 2019-11-07 07:35:22 | 2019-11-07 07:35:22 | Success |
| 5dc3866c944ef91eaad8392b | servicesReauth | 172.16.0.86 | 2019-11-07 09:50:20 | 2019-11-07 09:50:20 | Success |
| 5dc50637944ef91eaad83a13 | activateService | 172.16.0.86 | 2019-11-08 13:07:51 | 2019-11-08 13:07:51 | Success |
| 5dc8fdca944ef91eaad83aab | servicesReauth | 172.16.0.86 | 2019-11-11 13:20:58 | 2019-11-11 13:20:58 | Success |
| 5dba55069dd77f7eee42a696 | activateService | 172.16.0.86 | 2019-10-31 10:29:10 | 2019-10-31 10:29:10 | Success |
| 5dba69109dd77f7eee42a6b5 | activateService | 172.16.0.86 | 2019-10-31 11:54:40 | 2019-10-31 11:54:40 | Success |

Information on the status of CoA requests between PCRF and BRAS is displayed on this tab. Entries can be filtered by NAS IP, command type, request (Queued) and execution (Complete) date.
CoA request logs for the following commands are available:

- URL list requery;
- Services requery;
- Data tunnel establishment;
- Domain properties update;
- Service activation;
- Service deactivation;
- Session termination.

## MAC bonds




On this tab, information on SoftWLC Hotspot subscribers' MAC addresses is displayed. Entries can be sorted by: last activity time, login, domain or subscriber's MAC address.
MAC addresses are used during MAC-based authorization of Hotspot users. Mac address storage time is specified in portal settings of the Portal Constructor. A user will not have to pass authorization on the portal during this period.
The following parameters are available on the tab:

- *Username* — a subscriber's login;
- *Domain* — a subscriber's domain;
- *MAC address* — a subscriber's MAC address;
- *Vendor* — a device manufacturer;
- *Expires* — an entry's expiration time.

## URL lists


URL list for BRAS are created on this tab.
A list may contain:

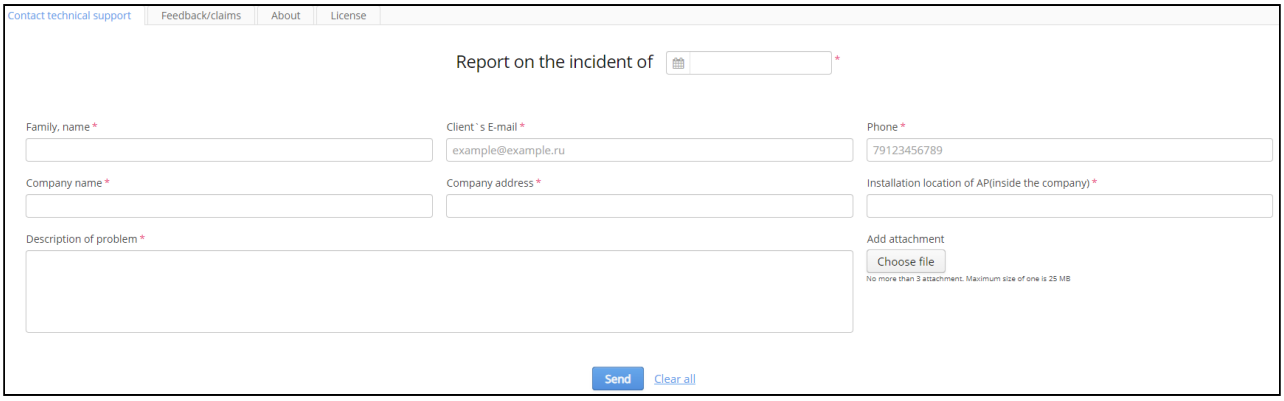
- URL addresses, data format: http://eltex-co.com/;
- Templates (regular expressions), data format: ^((https|http):\/\/)(.+\.)?eltex-co\.ru;
- IP/MASK, data format: 192.168.0.0/24;
- IP/MASK (TCP), data format: 192.168.0.0/24. Used for applications operating on HTTP/HTTPS ports but do not transfer HTTP/HTTPS data.

A list has the limitations:

1. no more than 5000 entries
2. no more than 255 characters in a string

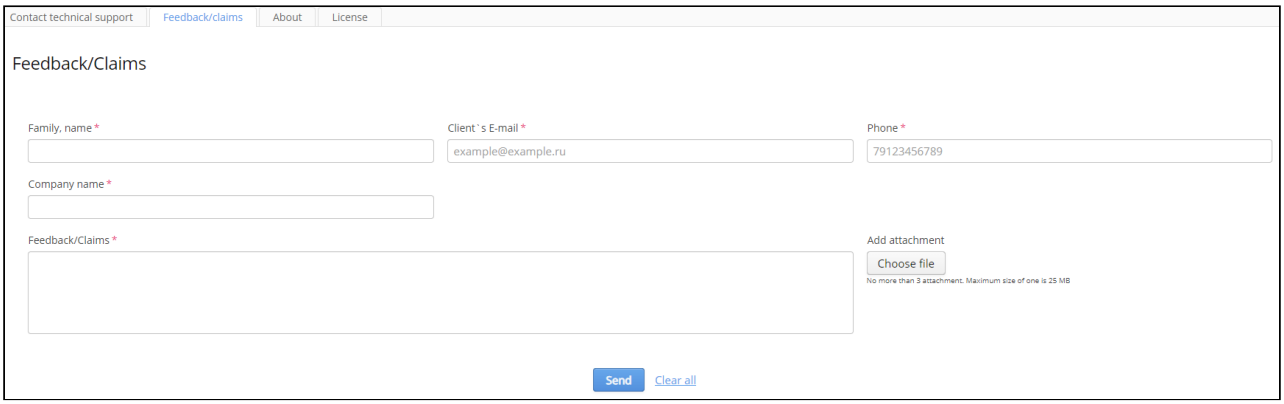
## Reference

### Contact technical support




The tab *"Contact technical support"* contains a form with obligatory fields to report a problem to a technical support.

### Feedback/claims



The tab *"Feedback/claims"* contains a form with obligatory fields to send a feedback/a claim to a technical support.

### About

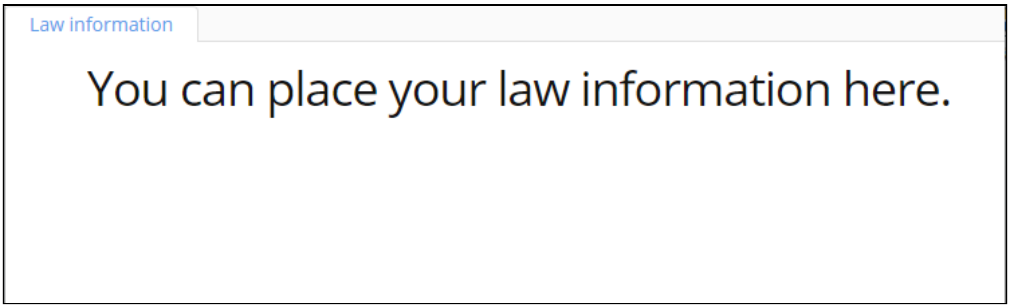
The tab *"About"* contains information on the Wi-Fi B2B Admin Panel version and contacts of a technical support service.

By default, contacts of a device vendor (i.e. ELTEX) are displayed. But in the provider's level scheme, contacts of a provider can be specified for its clients (providers working with legal entities) to address the provider instead of the vendor. This can be done on the tab *"System" -> "Client"* of the *"Settings"* section. A provider should put data in the field *"Technical support data"*.

### License

This section contains information on licenses for the system "Wi-Fi B2B Admin Panel" and PCRF.

### Law information




Legal information can be placed in this section.

## v1.14_Admin Panel administration (EN)

- Configuration files

- GUI settings
  - System
    - System
    - Integration
    - Tables
    - Notifications
    - B2B clients notifications
    - Client
    - Creating a domain
    - Editing a domain
    - Deleting a domain
  - System users
    - Adding a user
    - Cloning a user
    - Sending notifications
      - Selecting a domain for a user
    - Editing a user
    - Deleting a user
  - System roles
    - Adding/editing a system role
    - Copying a role
    - Deleting a role
  - Server addresses
    - Adding a user
    - Editing a user
    - Deleting a user
- Licensing
  - Licensing procedure and installation
  - Checking a license


## Configuration files

The file **/etc/eltex-wifi-cab/system.xml** contains settings to connect to MongoDB, NBI and authorization service.

- Connecting to MongoDB:

```
    <entry key="mongoaddress">mongodb://localhost:27017/wifi-customer-cab</
entry>
```

- Connecting to NBI (address, login, password):

```
    <entry key="nbiaddress">http://localhost:8080/axis2/services/
RadiusNbiService?wsdl</entry>
    <entry key="nbi.serviceLogin.user">softwlc_service</entry>
    <entry key="nbi.serviceLogin.password">softwlc</entry>
```

- Connecting to Admin Panel users authorization service:

```
<entry key="radius.auth.address">localhost</entry>
<entry key="radius.auth.shareSecret">testing123</entry>
<entry key="radius.auth.authPort">21812</entry>
<entry key="radius.auth.acctPort">21813</entry>
```

## GUI settings

The section *"Settings"* contains general settings of Wi-Fi B2B Admin Panel and allows creating its roles and users lists, configuring domains and interacting with other platform elements.

The section *"Settings"* contains 6 tabs:

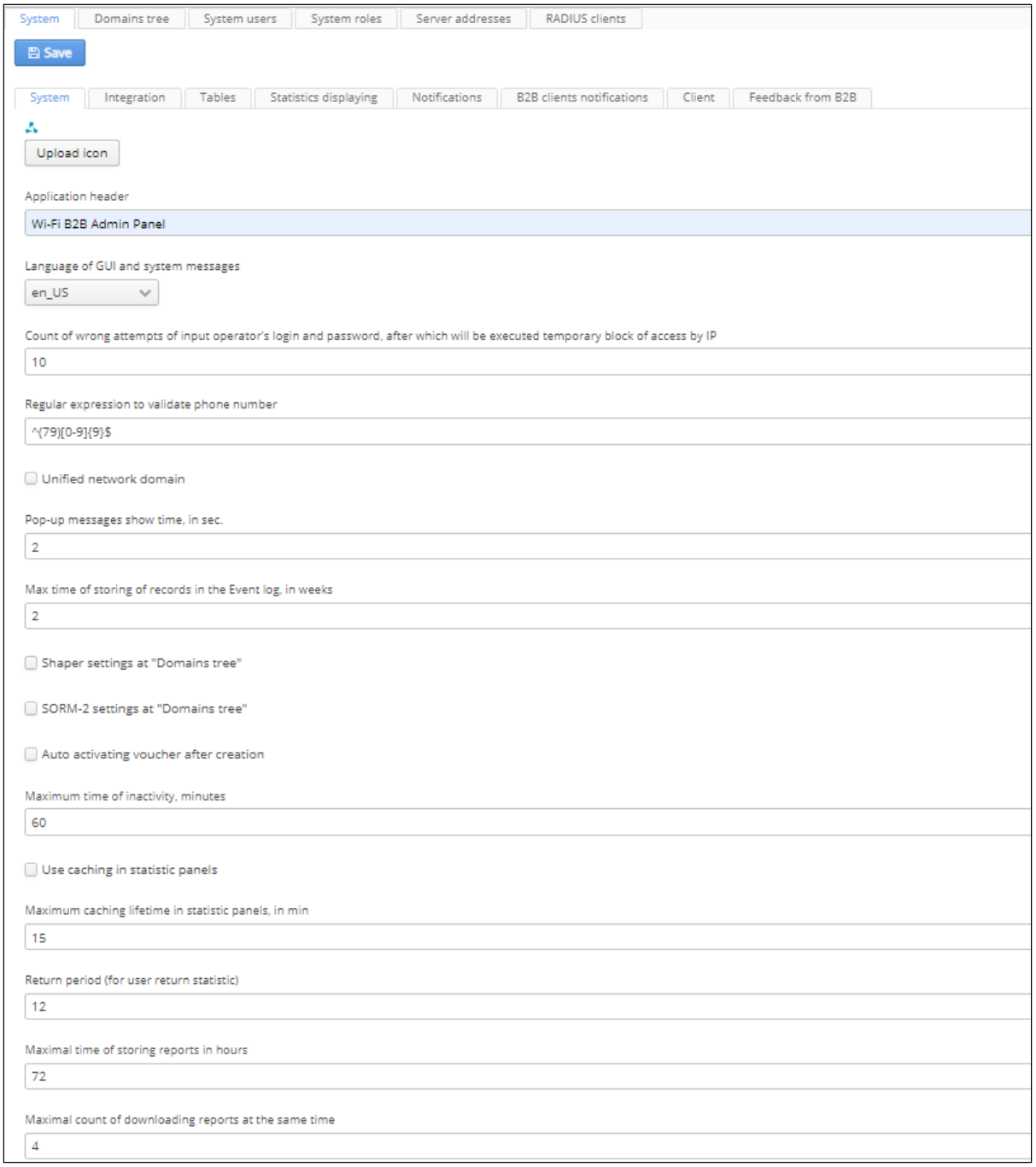
- *"System";*
- *"Domains tree";*
- *"System users";*
- *"System roles";*
- *"Server addresses";*
- *"RADIUS clients".*

Each tab is responsible for a certain group of settings. An opportunity to edit most settings is available only for a user with the role of a system administrator.

### System

To save changes, click the button *"Save",* located at the top of the page. Settings are applied immediately, service restart is not needed.

### System



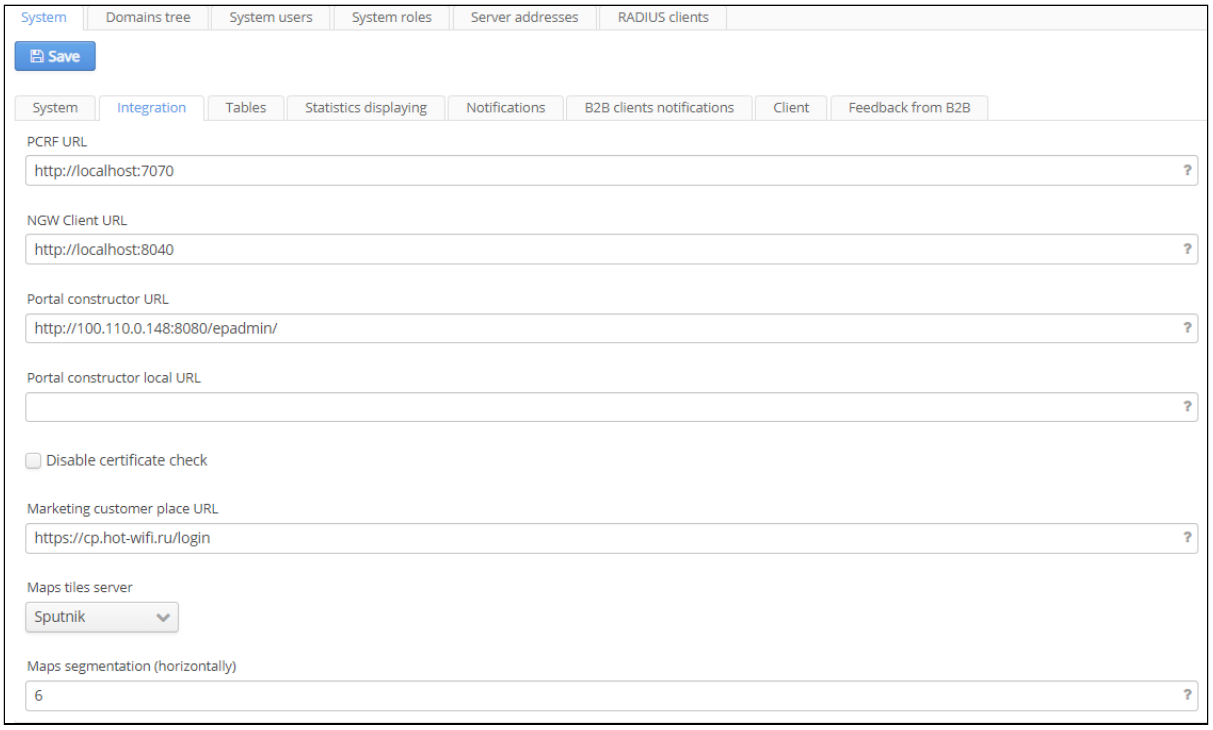

The tab *"System"* is the main tab for the Wi-Fi B2B Admin Panel configuration.

- **Upload icon** — allows uploading a favicon for the Admin Panel.
- **Applicaton header**— allows specifying a header for the page in a browser.
- **Language of GUI and system messages** – 2 languages are available: English (en-US), Russian (ru_RU). For GUI changes to be applied, pass authorization again.
- **Count of wrong attempts of input operator's login and password, after which a temporary block of access by IP will be executed** – the parameter keeps the number of invalid inputs upon

exceeding of which an opportunity to enter credentials will be stopped for 10 minutes (password sniffing protection).

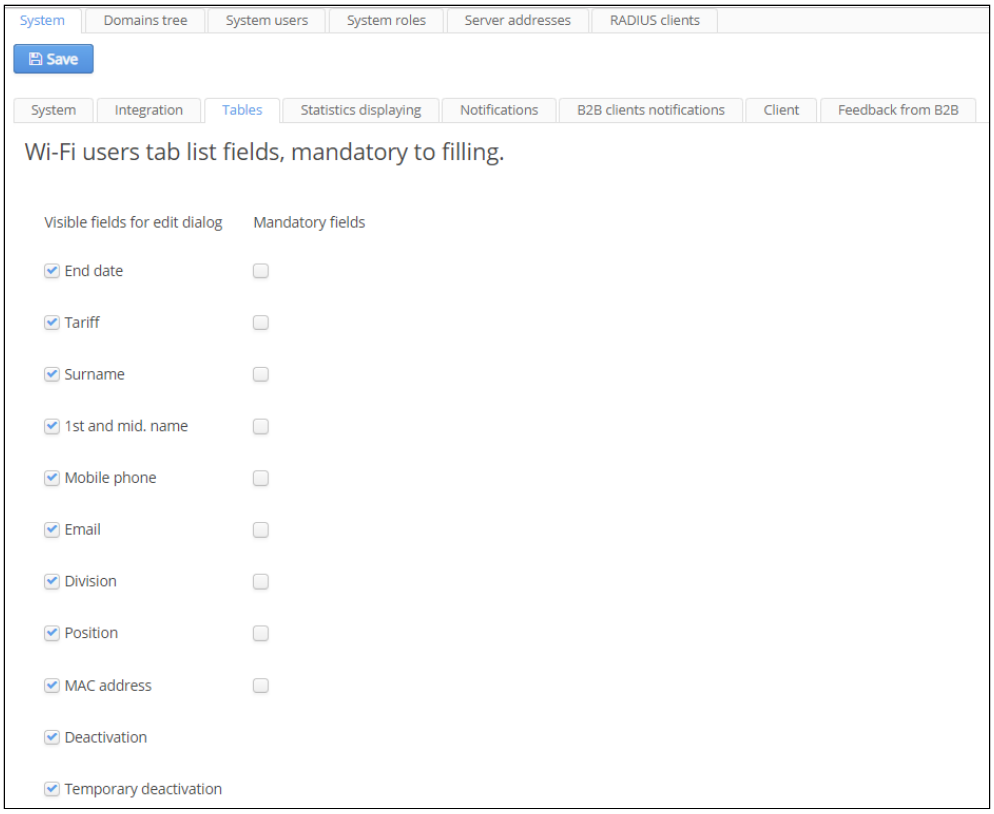
- **Regular expression to validate phone number** – allows specifying a regular expression to validate phone number when creating a Wi-Fi user. The system comes with a regular expression that allows only mobile phone numbers in the international format.
- **Unified network domain –** used when there are no subdomains in the system. When checked, all user accounts will be located in the root domain. The mode makes working with the interface easier when the system is used to service one organizations without subsidiaries.
- **Pop-up messages show time –** a time period (in seconds) during which a warning pop-up window is displayed.
- **Max time of storing of records in the Event log, in weeks**– the maximum possible number of events in the event log. On exceeding of this limit, old entries will be deleted. By default, this period is two weeks.
- **Shaper settings at "Domains tree –** enabling shaper settings on access poins installed within the same domain the Domains tree. Shaper data work when there is a link between SoftWLC and ESR-1000 (SoftWLC configures shapers on ESR-1000 to which the group of access points is connected).
- **SORM-2 settings at "Domains tree" –** enabling the setting for RADIUS traffic sending for SORM-2.
- **Auto activating voucher after creation –** automatic activation of vouchers after creating. If the option is not enabled, all created vouchers will be deactivated. To activate them, fill in the fields "Login" + "Phone number" or "Passport data".
- **Maximum time of inactivity –** a timeout upon exceeding of which a user is logged out. If a user performs some actions in the Admin Panel, the idle time counter is reset.
- **Use caching in statistics panels –** allows saving statistics samplings in order not to gather data again when switching the tabs.
- **Maximum caching lifetime in statistic panels, in min –**statistics cache storage time.
- **Return period (for user statistics).**
- **Maximal time of storing reports in hours –** time period during which reports are stored on the server. On exceeding this timeout, a report requested by a user will be deleted.
- **Maximal count of downloading reports at the same time –** if this number is exceeded, new users that try to download a report will have to wait.
- **Show ICMP diagram –** when checked, an opportunity to view diagrams showing ICMP results on device accessibility in the tab "Access points".
- **Show SNMP diagram –** when checked, an opportunity to view diagrams showing SNMP results on device accessibility in the tab "Access points".

Integration



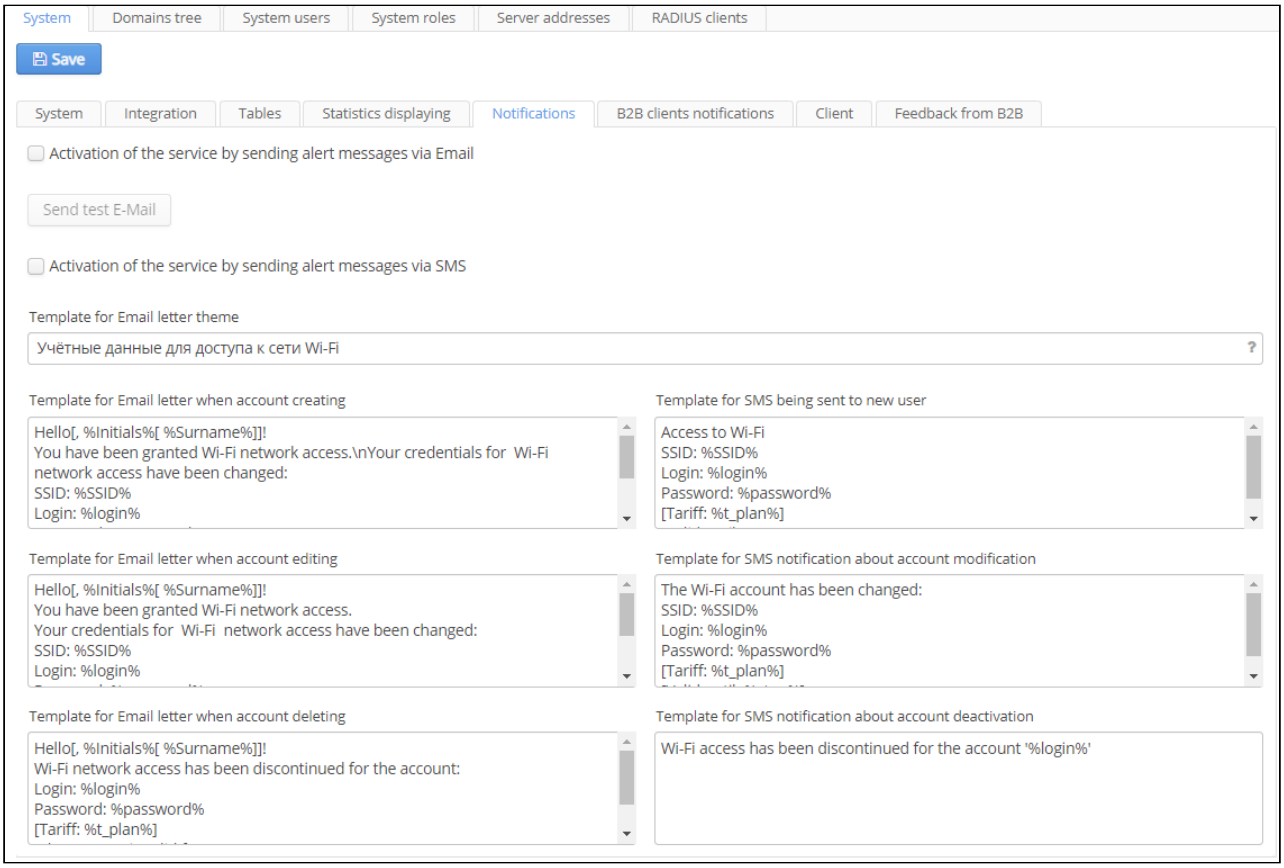

- **PCRF URL –** ELTEX-PCRF address.
- **NGW Client URL –** address of eltex-ngw service to send notifications via SMS or e-mail.
- **Portal constructor URL –** Portal Constructor address available for users from an external network. The parameter is applied for users to access the Portal Constructor.
- **Portal constructor local URL –** Portal Constructor address available within the core (from the Admin Panel server). Used to pass users' credentials to the Portal Constructor. If this address is equal to **Portal constructor URL**, leave this field empty. Interaction is carried out via HTTP.
- **Disable certificate check –** disables HTTPS certificate check when a user goes to the Portal Constructor.
- **Marketing customer place URL –** advertising platform address. Is used to move to advertising platform personal account.
- **Maps tiles server** – selecting a service that provides maps to which access points' locations will be projected.
- **Maps segmentation** – configuring a grid used for access points grouping when a scale is changed. When the number of segments is decreased, access points are clustered in sparse groups, the number of groups on the map decreases. When the number of segments is increased, groups become smaller, and the number of them increases. Valid values are between 3 to 30, recommended ones are from 6 to 12.

Tables




Configuring the fields that are obligatory when creating Wi-Fi users' accounts.

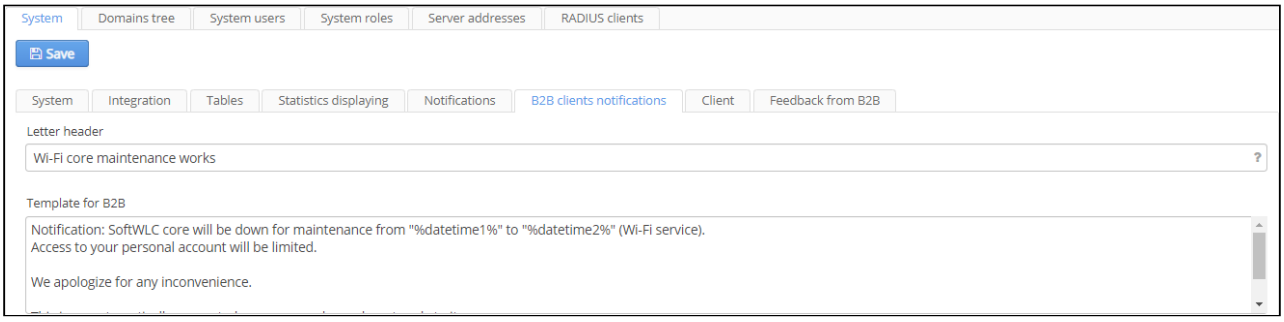
## Notifications




In this section, sending e-mail and SMS notifications to users is configured. To enable the service, check an appropriate checkbox.

- **Template for Email letter theme** – a title of letters sent to Wi-Fi users.
- **Template for Email letter when account creating** — allows specifying a text of a letter sent on account creation.
- **Template for SMS being sent to new user** – allows specifying a text of an SMS sent on account creation.
- **Template for Email letter when account editing** –allows specifying a text of a letter sent on account editing.
- **Template for SMS notification on account modification –** allows specifying a text of an SMS sent on account editing.
- **Template for Email letter when account deleting** – allows specifying a text of an SMS sent on account deletion.
- **Template for SMS notification about account deactivation** – allows specifying a text of an SMS sent on account deletion.

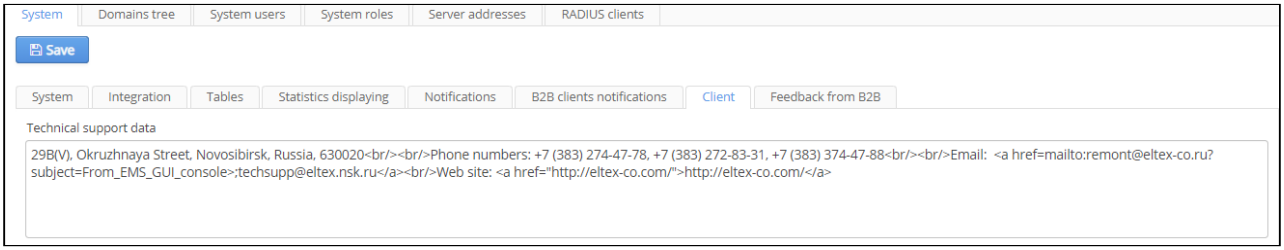
B2B clients notifications




In this section, notifications on platform maintenance (causing access interruptions) that are sent to Admin Panel users (for Platform administrators and B2B clients having Admin Panel user accounts) are configured.

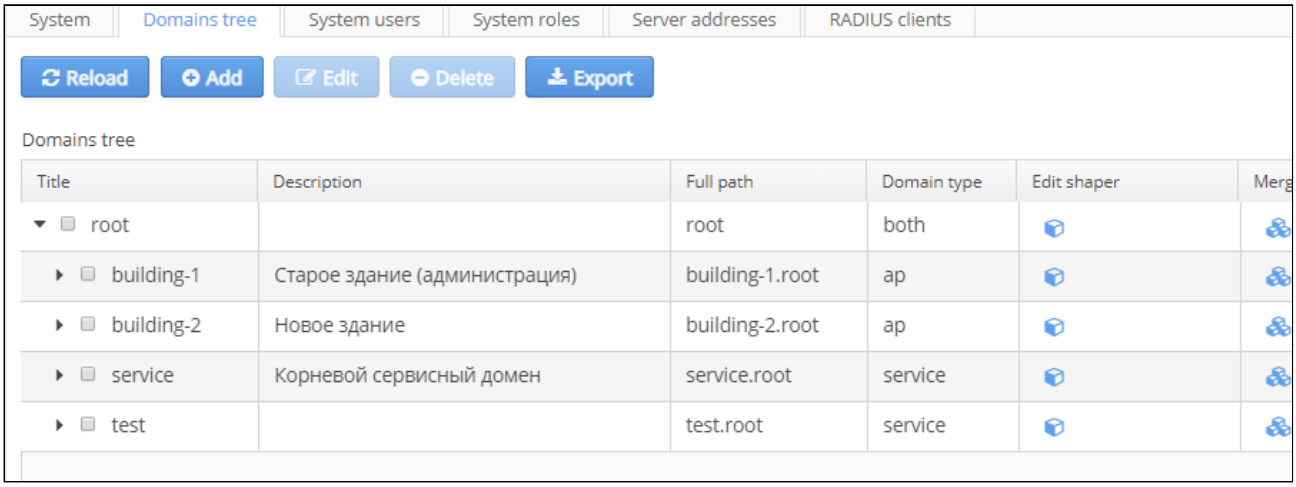
- **Letter header** – a header of a letter sent to Admin Panel users.
- **Template for B2B** – a template for a letter notifying of platform maintenance.

Client




**Technical support data** – allows specifying a text displayed on the page *"About"*.

Domains tree




In this section, the Wi-Fi platform domains are managed.

**Domains** – string identifiers by which separation of access rights for SoftWLC monitoring and management is performed.

Domains structure – a hierarchy according to which parent elements contain child elements. A first-level domain is called a root domain. For federal-level projects, the domain "root" is recommended.

A domain name should consist of digits and Latin letters. A length of each element should not exceed 63 symbols. Total length of a domain in string representation should not exceed 255 symbols. A point should be a separator (in string representation).

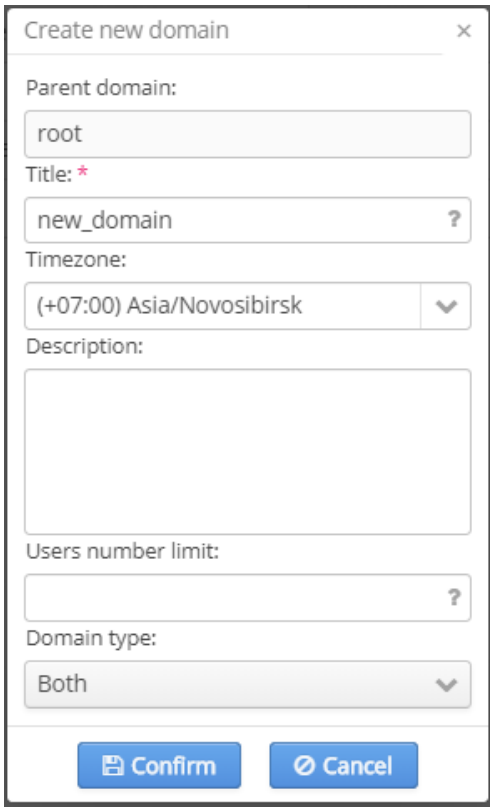
⚠ A root domain is specified by a system administrator during installation and cannot be replaced with another one later!

A table presented in the interface allows viewing a structure and elements of a domain tree.

A domain of a Wi-Fi user implies that a user belongs to a group and serves as a part of a pair login@domain that is a unique identifier of a user account within the Platform.

There are three types of domains in SoftWLC: Ap, Service, Both. If it is required to put access points and Wi-Fi users into different domains, access points should be put into domains with "Ap" type, and users should be put into domains with "Service" type. If there is no such a need, access points and Wi-Fi users should be put into a domain with "Both" type. Separation of access points and Wi-Fi users allows more flexibility in providing statistics data access within a big project.

Creating a domain



When the button *"Add"* is clicked, a dialog window for adding a new domain that contains a defined set of parameters is opened. *"Title", "Description", "Users Number limit".* Parameters marked with "*" are obligatory. An attempt to save an entry with obligatory fields that are not filled in or filled in incorrectly will be rejected. Problem fields will be highlighted red.

- *Title*– domain name (it should be consistent with the rules described above);
- *Description* – free form description of a domain. The description will be displayed in widgets on other pages of the Admin Panel;
- *Users number limit* — the maximum number of Wi-Fi users that can be located in a certain domain or its subdomains. The parameter allows setting quotas on the number of service users for organizations' departments, subsidiaries or client organizations.
- Domain type — defines domain type.
- Timezone — domain timezone. The parameter is used to define a timezone where access points are installed. For example, it is required for scheduled operation of the portal.

When the number of Wi-Fi users in a domain or a subdomain is modified, the program interface verifies that the total number of subdomain users is not higher than the total number of domain ones. A warning message is displayed on the screen. The interface does not allow creating subdomains with quotas higher than their parent domains' quotas.

The following command buttons are available in the dialog for domain adding/editing:

- *Confirm* — confirm the changes;
- *Cancel* — cancel the changes.

Editing a domain

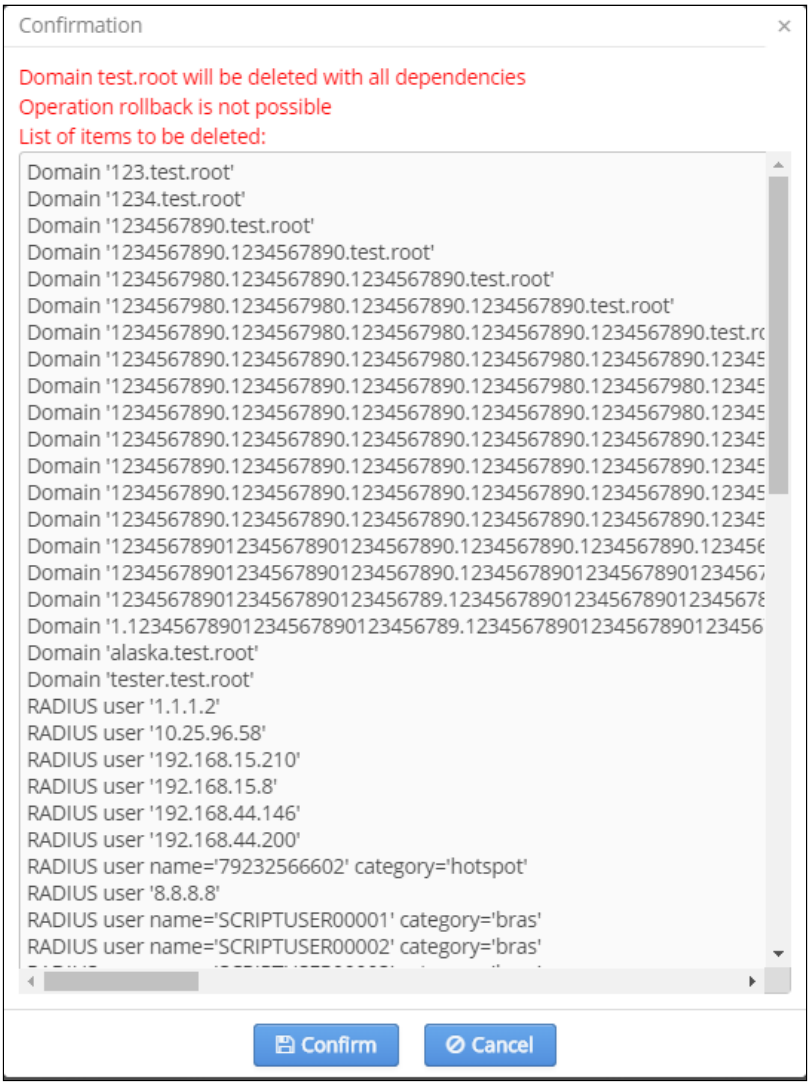
To edit a domain, select it from the table and click *"Edit"*. A corresponding window will be opened. The following parameters can be edited: *"Timezone", "Description"* and *"User Number limit".*

> Beginning from the version 1.10, a domain name cannot be edited after its creation! Domain name change can be performed only by deleting a domain and creating it again.

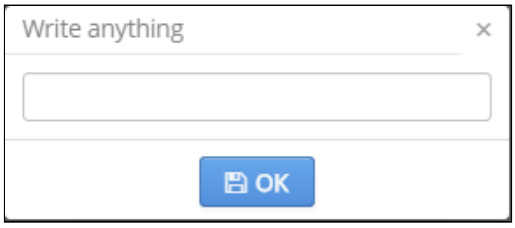
**Deleting a domain**

> Beginning from the version 1.9, domain deletion is available only for users with the role of SoftWLC platform administrator for security purposes.

To delete a domain, select it and click *"Delete"*. A domain can be deleted only with all its parameters. Confirmation via entering a user account password is required.
When the button "Delete" is clicked, a warning with all domain entries to be deleted is displayed:



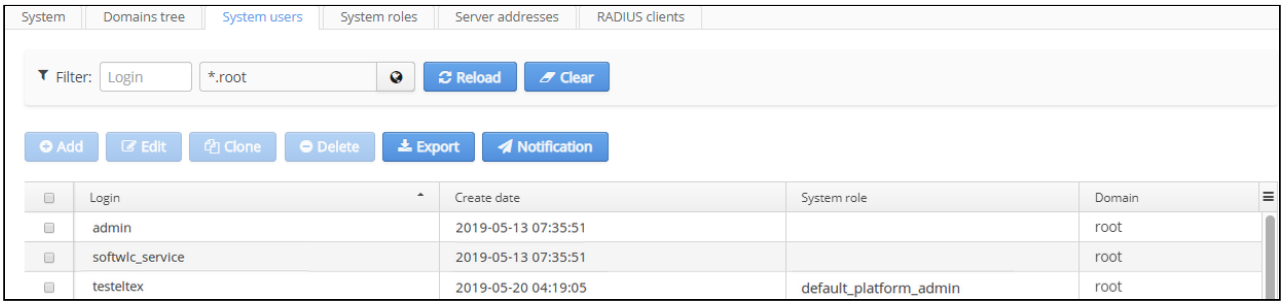

After clicking the button "Confirm", a password dialog will be displayed to confirm the operation.




If OK is clicked, a domain and all entities belonging to it (SSID, users, virtual portals, tariffs and others) will be deleted permanently.

Domain list visibility is limited to a domain of an operator. An operator of a subsidiary or an organization can view and manage only entries of its domain or subdomain. Entries of other domains are not available.

### System users

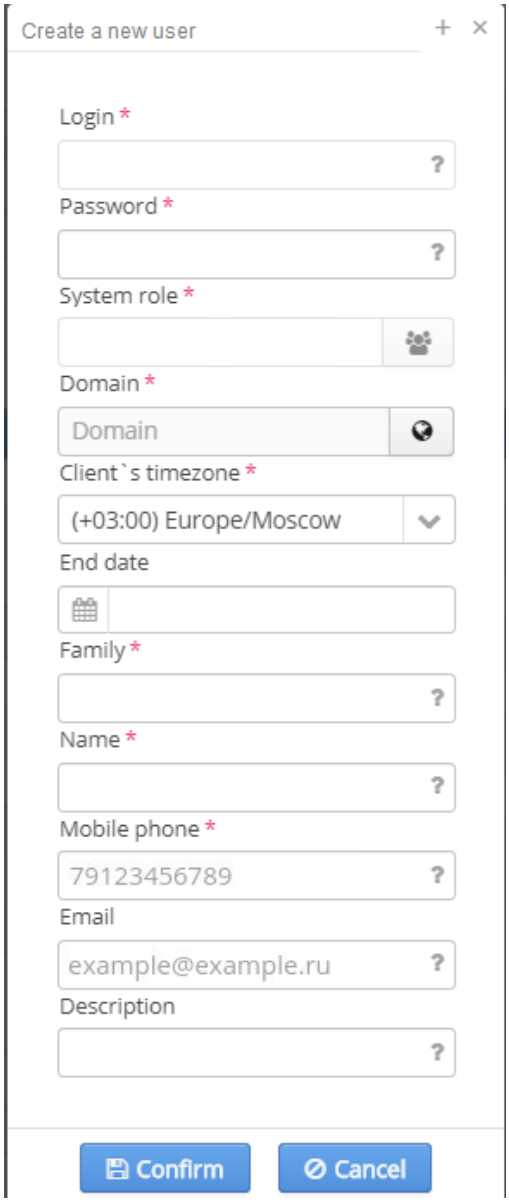



The tab *"System users"* is implied to manage users (operators) of services included into SoftWLC. User accounts configured in this tab are used to access the Wi-Fi B2B Admin Panel and the Portal Constructor.

The tab allows creating, deleting and cloning accounts of system operators. If lists are long, it is convenient to use filters.

User list visibility is limited to a domain. An operator of a subsidiary or an organization can view and manage only entries of its domain or subdomain. Entries of other domains are not available.

#### Adding a user



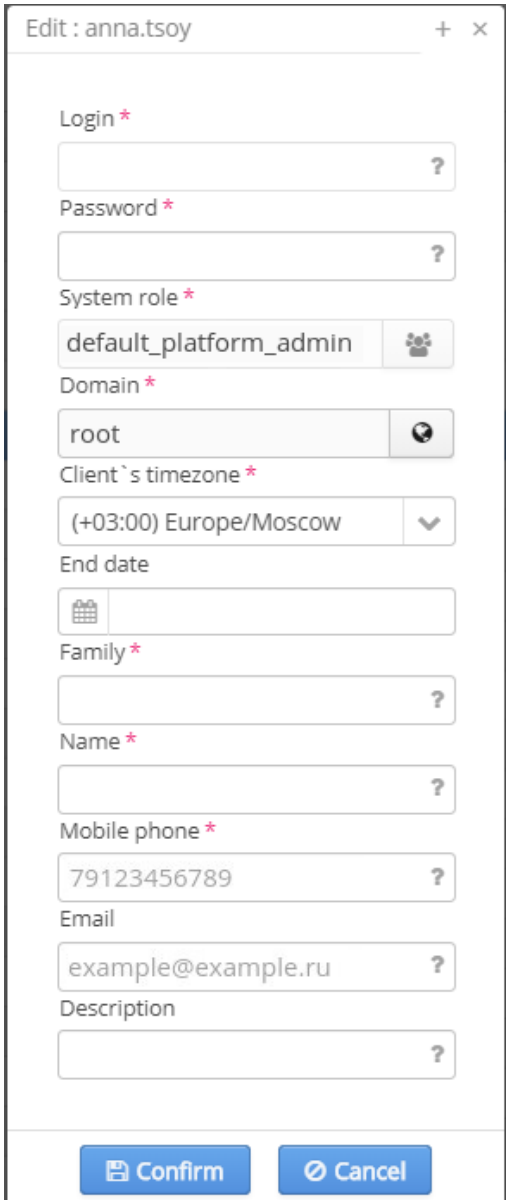

When the button *"Add"* is clicked, a dialog window for adding a system user that contains a defined set of parameters is opened. All the parameters are obligatory. An attempt to save an entry with obligatory fields that are not filled in or filled in incorrectly will be rejected. Problem fields will be highlighted red. When a mouse is over a field, a prompt is displayed.The set of parameters:

- *Login* — the parameter is used as a unique identifier to enter the systems "Wi-Fi B2B Admin Panel" and "Portal Constructor";
- *Password* — a unique password to a user account;
- *System role* — user account belonging to one of the system roles;
- *Domain* — a domain to which a user will be added. Each user can have several domains.
- Client's timezone — all data will be displayed according to a timezone.
- End date — user account expiry date after which it cannot be used for authorization.

- Family/Name — additional user account parameters. The need for their usage is configured an the Admin Panel. The Admin Panel records by whom a Wi-Fi user account was created and edited.
- Mobile phone — a phone for notifications sending.
- Email — e-mail address for notifications sending.
- Description — information on an account.

> ⚠ One user account can have only one system role but several domains.

Cloning a user

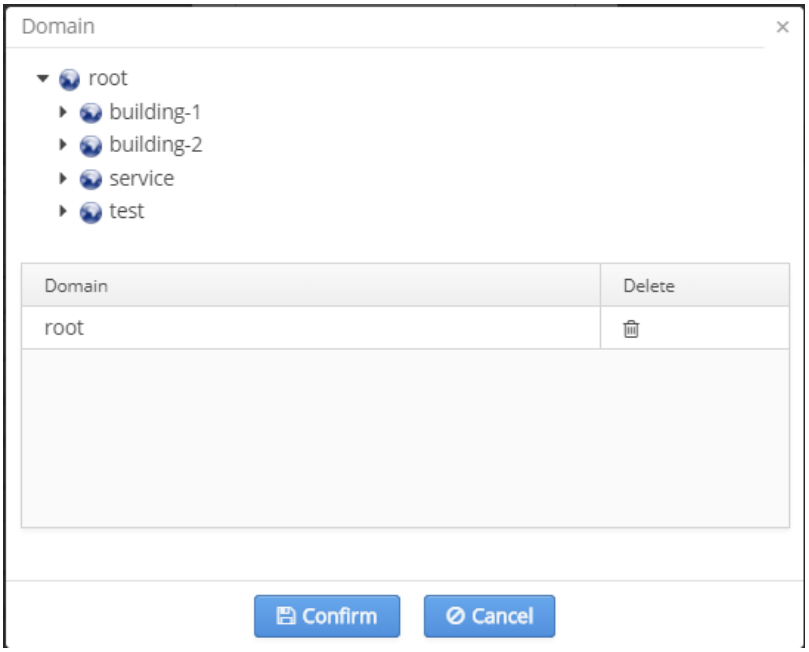


When the button *"Clone"* is clicked, a dialog window for cloning a system user that contains a defined set of parameters is opened. The parameters "System role", "Domain" and "Client's timezone" are copied from the account to be cloned. The other parameters are specified manually.

### Sending notifications

When the button *"Notification"* is clicked, a dialog window for sending e-mail notifications containing a message template specified in the menu *"B2B clients notifications"* is opened. In this window, a message can be edited for a certain case, and a domain to which a message will be sent can be selected.

### Selecting a domain for a user




To select a domain for a user, a special widget showing a domain tree and a list of added domains is implemented.

- To add a new domain, select it in a tree.
- To delete a domain, click the icon  .

Editing a user

When a checkbox on the left side of the table is checked for an entry, the button *"Edit"* is enabled. Click this button, and a dialog window similar to one for creating a user but including additional information on account creation date will be opened.

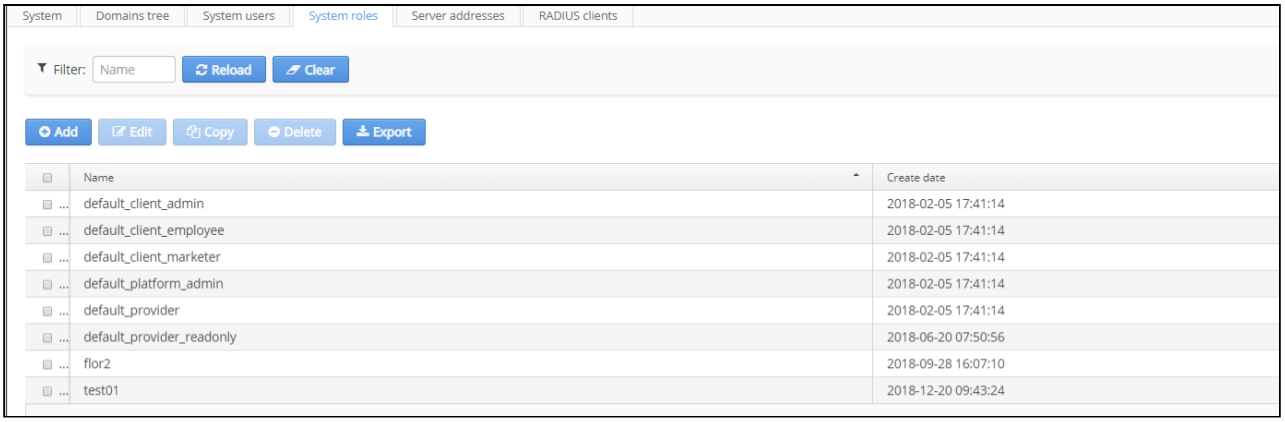
A user's login cannot be edited because the field "Login" is an entry identifier. If required, an entry can be deleted and created again.

### Deleting a user

To delete an entry, check a corresponding checkbox and click *"Delete"*. Thus, several entries can be selected and deleted simultaneously. If the checkbox in the table header is checked, the whole table will be selected.

Unable to delete "admin". Users cannot delete their own accounts, i.e. the accounts under which they enter the system.

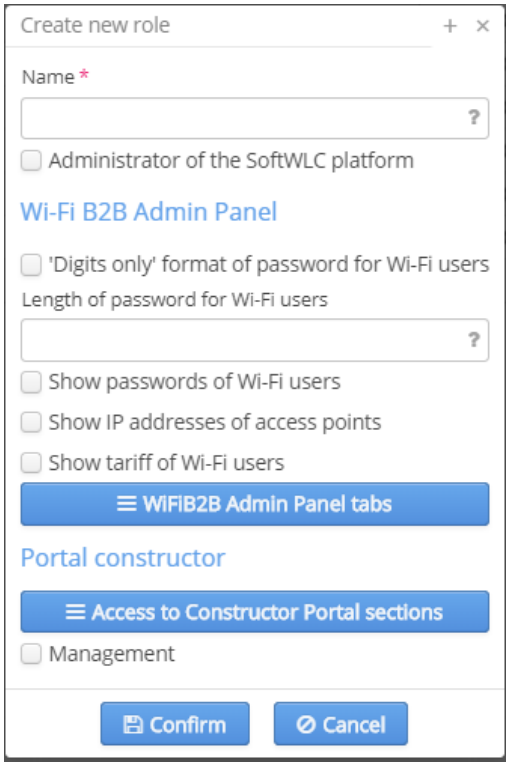
### System roles




The tab *"System roles" is used* to configure management roles. Role is a set of attributes that allows structuring the Wi-Fi B2B Admin Panel users' (operators') rights and simplifying rights configuration.

Each system role has a name, a set of main attributes defining user rights in the systems "Wi-Fi B2B Admin Panel" and "Portal Constructor" and an expanded list of attributes that specifies user rights for each page of a system. All these allow creating a flexible Platform resources management scheme. For example, there is an opportunity to configure roles of Platform super user, telecommunication provider, company client etc. There can be a local administrator within each group (with rights that do not extend beyond their domain), operators with "read" access and operators with "read and write" access to any platform resources.

### Adding/editing a system role




When the button *"Add"* is clicked, a dialog window for adding a system role that contains a defined set of parameters is opened. Fields marked with "*" are obligatory. An attempt to save an entry with obligatory fields that are not filled in or filled in incorrectly will be rejected. Problem fields will be highlighted red. When a mouse is over a field, a prompt is displayed.
The following command buttons are available:

- *Confirm* — confirm the changes;
- *Cancel* — cancel the changes.

The privileges given to system roles are described in the section Description of Admin Panel and Portal Constructor users' privileges

### Copying a role

Instead of creating a role from scratch, roles created before can be used. To do that, select a role and click "Copy".

A window similar to the role creating/editing one will be opened. A new name should be specified, and required parameters should be changed in it.

### Deleting a role

To delete a role, select it and click "Delete". If a role is not used by existing users, it will be deleted after confirmation.

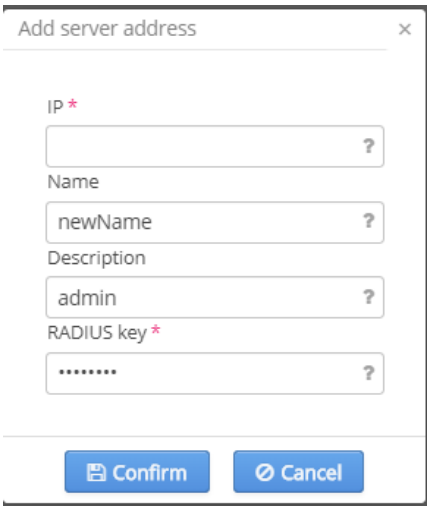
## Server addresses


In the tab *"Server addresses"* an interface for registration of host addresses in multi-server installations is provided. IP addresses of all servers used for platform users authentication should be added to the table. That is, they are main and reserve addresses of hosts on which the systems "Wi-Fi B2B Admin Panel" and "Portal Constructor" are installed.

When all services are running on the same host and communicate via "localhost", address registration is not needed.

If the system is installed on several hosts, a primary address of a server with the "Wi-Fi B2B Admin Panel" installed can be specified via Eltex.EMS under super admin.

## Adding a user




When the button *"Add"* is clicked, a dialog window for server address editing that contains a defined set of parameters appears. Fields marked with "*" are obligatory. An attempt to save an entry with obligatory fields that are not filled in or filled in incorrectly will be rejected. Problem fields will be highlighted red. When a mouse is over a field, a prompt is displayed.

## Editing a user

When a checkbox on the left side of the table is checked for an entry, the button *"Edit"* is enabled. Click this button, and a dialog window for server address configuration will be opened. The window is described in the section *"Adding a user"*.

#### Deleting a user

To delete an entry, check a checkbox in a corresponding row and click *"Delete".* Deleting several entries simultaneously is available.

### Licensing

The number of users that can be logged in the Admin Panel and work with its WEB interface simultaneously is limited by licenses.

Administrative accounts ('admin','softwlc_service') are not included in the total number of logged in users when new accounts are created. However, they are included there when the number of simultaneous website visitors is calculated (when entering Admin Panel).

#### Licensing procedure and installation

A license file is not included into eltex-wifi-cab package by default. In this mode, a demo license for 5 users can be used to evaluate the system.

Eltex specialists will generate a personal license file and create a e-Token key in the acquisition of licenses.

E-Token should be connected to a server's USB interface. If a server operates on a virtual machine, the key should be forwarded to a virtual machine.

The license file should be put into the following directory:

```
/etc/eltex-wifi-cab/
```

After that, tomcat service should be restarted.

#### Checking a license

To check if licenses have been applied successfully, select "License" in the "Help" tab of GUI EMS. Information on the current license and the maximum number of users is available in the tab.

## v1.14_Description of Admin Panel and Portal Constructor users' privileges (EN)


- Role attributes
  - SoftWLC platform administrator
  - Admin Panel
    - Additional role parameters

- 'Digits only' format of password for Wi-Fi users
- Length of password for Wi-Fi users
- Show passwords of Wi-Fi users
- Show IP addresses of access points
- Show tariff of Wi-Fi users
- WiFi B2B Admin Panel tabs
- Portal Constructor
  - Virtual portals management
  - Access to Portal Constructor sections
    - Gallery
    - Advertising platforms
    - System settings
    - Payment service
    - Appearance
    - Security settings
    - Common settings
    - Language settings
    - Tariffs
- Description of the Admin Panel and the Portal Constructor users' default roles
- Converting roles to the default set


## Role attributes

### SoftWLC platform administrator

The privilege implies full access to the system including Admin Panel and Portal Constructor system settings.

### Admin Panel

### Additional role parameters

| Attribute | Description |
|---|---|
| 'Digits only' format of password for Wi-Fi users | When checked, only digits can be used for Wi-Fi users' passwords. |
| Length of password for Wi-Fi users | Minimum length of Wi-Fi users'passwords. |
| Show passwords of Wi-Fi users | Permission to view passwords to Wi-Fi users' accounts. |
| Show IP addresses of access points | When checked, an additional column containing IP addresses of access points is displayed in the table of access points. |
| Show tariff of Wi-Fi users | Permission to view tariffs in Wi-Fi users' accounts. |

WiFi B2B Admin Panel tabs

There are several privilege levels:

 - this option is not available for the user

 - permission to view

 - permission to edit

| Section | Page | Description |
|---|---|---|
| Services and tariffs | Tariffs | Setting tariffs for Wi-Fi users connection |
| | PCRF services | Configuring services used in BRAS (PCRF) tariffs |
| | PCRF scenarios | Configuring scenarios used in BRAS (PCRF) |
| Wi-Fi users | Enterprise Users | The table of 'enterprise' users that authorize on Eltex access points via EAP (RADIUS) |
| | Hotspot users | The table of 'hotspot' users that authorize on Eltex and other access points via BRAS (PCRF) using Eltex.Portal. |
| | Vouchers | The table of randomly generated users. |
| | Blocking Account | Configuring black lists of MAC addresses. |
| | Block by def | Configuring access lists of clients' phone numbers |
| | Top active users Enterprise | Monitoring and blocking of Enterprise users with maximum traffic consumption |
| | Top active users Hotspot | Monitoring and blocking of Hotspot users with maximum traffic consumption |
| Event log | Event log | System events log |
| | Wi-Fi users event log | The log contains Wi-Fi users' accounts changes parformed by system administrators |
| Scheduler | Scheduler | Scheduled operations management |
| Reference | Contact technical support | Tech support request form |
| | Feedback/claims | Feedback/Claim submit form |
| Access points | Devices | The table contains a list of access points and consolidated information on them |
| | Problem devices | The table contains a list of emergency (unavailable) access points |
| | Offices status | The table contains integrated figures and status of offices with access points installed |
| | Map | The map on which access points are displayed according to their geodata. |

| | | |
|---|---|---|
| SMS statistic | SMS statistic by time | The page with charts showing SMS sent at specific times. |
| | SMS statistic by group | The table with SMS sending statistics |
| | Outgoing SMS | The table showing sent SMS and their status. |
| PCRF settings | L2 subnetworks | L2 subnetworks are created in this tab |
| | PCRF info | Information on CoA requests status and BRAS sessions statistics |
| | CoA log | Information on CoA requests status between PCRF and BRAS |
| | MAC addresses | Information on clients' MAC addresses |
| | URL lists | URL lists for BRAS |
| Statistic of a provider | Quotas | Information on Admin Panel users |
| | Summary data | General information about the system state |
| | Graphic | Information on the Wi-Fi platform operation in graphic form |
| | Session statistic profile | The table contains information on Wi-Fi users' sessions |
| | SSID Groups | Information on the whole network in relation to SSID |
| | AP groups | Statistics on access points groups |
| | Access points | Information on a status of access points installed on the network |
| | Confirmation methods | Statistics on Wi-Fi users authorization ways |
| Advertising platform | Advertising platform | Configuring integration with advertising platforms |
| Enterprise statistics | Traffic | Traffic statistics for 'enterprise' users |
| | User sessions | Session statistics for 'enterprise' users |
| Hotspot statistics | Users | Statistics on the number of 'hotspot' users |
| | Service | Statistics on providing 'hotspot' users with services |
| | Traffic | Traffic statistics for 'hotspot' users |
| | Re-visits | Statistics on 'hotspot' users' revisits |
| | User sessions | Session statistics for 'hotspot' users |
| Portal Constructor | Portal Constructor | The button to go to the Portal Constructor from the Admin Panel |
| Wireless networks | Wireless networks | The section for SSID wireless networks configuration |

| | | |
|---|---|---|
| Settings | System users | Configuring accounts for Admin Panel and Portal Constructor users |
| | System roles | Configuring roles for Admin Panel and Portal Constructor users |
| | RADIUS clients | NAS table for eltex_auth_service |

Portal Constructor

Virtual portals management

The privilege gives the right to create, delete or edit virtual portals' names and domains.

Access to Portal Constructor sections

There are several privilege levels:

 - this option is not available for the user

 - permission to view

 - permission to edit

Permission to view is given to any user by default.

| **Section** | **Description** |
|---|---|
| Gallery | This option gives an opportunity to work with the image gallery. Even if the option is unavailable for a user, images from the gallery can be used for virtual portals configuration. |
| Advertising platforms | Access to advertising platforms configuration. This section is located in virtual portal settings. |
| System settings | The option allows changing Portal Constructor system settings. This privilege should not be given to average users. |
| Payment service | This option gives rights to configure integration with payment services. The section is located in virtual portal settings. |
| Appearance | Access to virtual portal appearance configuration. Since it is the main user function,the privilege is automatically added to any role, at least at a minimal level (viewing). |
| Security settings | CAPTCHA algorithms and Wi-Fi users access lists settings. These settings are located in the section "Common settings". |
| Common settings | Virtual portal settings section comprising specific parameters of each portal such as MAC address storage time, Mode, Additional pages. Antispam settings are also located there. |

| | |
|---|---|
| Language settings | The option for portal settings that are specific for each language and not related directly to appearance. For example: SMS template, Redirection URL, Page titles.<br>The section is located in virtual portal settings. |
| Tariffs | Access to portal tariffs configuration. The section is located in virtual portal settings. |

## Description of the Admin Panel and the Portal Constructor users' default roles

A role is a set of attributes that allows structuring of the Wi-Fi B2B Admin Panel users' (operators') rights and simplifying rights configuration.Each system role contains a set of main attributes defining user rights in the systems "Wi-Fi B2B Admin Panel" and "Portal Constructor" and an expanded list of attributes that specifies user rights for each page of a system. All these allow creating a flexible Platform resources management scheme.
A set of default system roles is provided for the Admin Panel. Each role is preset for a user to be able to deal with necessary tasks.

| | | |
|---|---|---|
| default_platform_admin | Platform administration | **Administrator of the SoftWLC platform**. The role implies access to all system elements. |
| default_provider | Adding new platforms for clients | **Provider's staff member**. Has rights to configure domains, tariffs, portals, roles and Admin Panel users. Wi-Fi users, all statistics. Does not have access to settings that have impact on the work of the system |
| default_client_admin | Customizing some aspects of the system | **A client's administrator**. Has rights to create new enterprise users, vouchers, virtual portals settings and to gather client statistics |
| default_client_marketer | Virtual portals customization | **A client's marketer**. Virtual portals configuration privileges, client statistics gathering |
| default_client_employee | Monitoring | **A client's staff member**. Viewing portals, statistics, lists of Wi-Fi users |
| provider_read_only | Monitoring | **A provider's staff member_read only.**Has permission to view domains, tariffs, portals, roles, Admin Panel users. Wi-Fi users, all statistics. Does not have access to settings. |

## Converting roles to the default set

In the version SoftWLC 1.8, domain settings are put into the System users tab instead of the System roles. It helps to get rid of excessive roles that were created for each client of a provider within the context of previous versions. Hence conversion of roles created before to the default set is needed. That allows making roles and users management easier.
To convert existing roles to the default set automatically, the special script 'auth-roles-converter' was created. The scripts changes user roles according to the following rules:

1. All roles having Admin Panel or Portal Constructor administration privileges (super users) are considered as equivalent to platform administrators. Users who had these roles get the role of the platform administrator (default_platform_admin). After that, an old role is deleted.
2. Remaining roles are compared with client roles according to the following order: 'default_client_employee', 'default_client_marketer', 'default_client_admin'. If one of the default roles contains all privileges of a converted role, they can be considered as equivalent. In this case, users get an equivalent role, and an old role is removed.
3. If roles are equivalent to no roles from the default set, all users having the role are assigned 'default_client_admin', an old role is also removed.
4. The role 'default_provider' is not assigned by the script.

When started, the script will display a role conversion plan and wait for a confirmation. After confirmation, backups of tables containing data on system roles will be created. After that, conversion will be performed. Restart 'eltex-auth-service' process and tomcat7 on servers with the Admin Panel and the Portal Constructor.

To perform roles converting, the script `auth-roles-converter` is used

When starting the script, specify login and password to access the database eltex_auth_service :

```
./auth-roles-converter -uroot -proot
```

During script execution, a list of offered changes will be displayed. If a decision to accept changes is made, a backup will be created, for example:

```
root@vagrant-ubuntu-trusty-64:/home/vagrant# ./auth-roles-converter -uroot
-proot
No replacement of default_provider2 with Eltex-Tab-Pcrf-Macs = 2. This role
will be replaced by default_client_admin
No replacement of providerdefault_ with Eltex-Tab-Pcrf-Macs = 2. This role
will be replaced by default_client_admin
Role client_admindefault_1 will be replaced with default_client_admin
Role client_employeedefault_ will be replaced with default_client_employee
Role client_marketerdefault_ will be replaced with default_client_marketer
Role default_client_admin2 will be replaced with default_client_admin
Role default_client_employee2 will be replaced with default_client_employee
Role default_client_marketer2 will be replaced with default_client_marketer
Role default_platform_admin2 will be replaced with default_platform_admin
Role default_provider2 will be replaced with default_client_admin
Role platform_admindefault_ will be replaced with default_platform_admin
Role providerdefault_ will be replaced with default_client_admin
Continue? [y/N] y
SQL Dump of tables: radgroupreply, radgroupcommon, radusergroup is located
at /home/vagrant/eltex_auth_service_backup.sql
Replaced role client_admindefault_1 with default_client_admin for 1 users
Replaced role client_employeedefault_ with default_client_employee for 1
users
Replaced role client_marketerdefault_ with default_client_marketer for 1
users
Replaced role default_client_admin2 with default_client_admin for 0 users
Replaced role default_client_employee2 with default_client_employee for 0
users
Replaced role default_client_marketer2 with default_client_marketer for 0
users
Replaced role default_platform_admin2 with default_platform_admin for 0 users
Replaced role default_provider2 with default_client_admin for 0 users
Replaced role platform_admindefault_ with default_platform_admin for 1 users
Replaced role providerdefault_ with default_client_admin for 1 users
root@vagrant-ubuntu-trusty-64:/home/vagrant#
```

where

```
Role client_admindefault_1 will be replaced with default_client_admin
```

That means that no appropriate equivalents have been found for 'default_client_employee2', and it will be converted into 'default_client_employee'

```
No replacement of default_provider2 with Eltex-Tab-Pcrf-Macs = 2. This role will
be replaced by default_client_admin
```

An appropriate replacement has not been found for 'default_provider2', it will be substituted by 'default_client_admin'

```
Continue? [y/N] y
```

Confirm the changes

```
SQL Dump of tables: radgroupreply, radgroupcommon, radusergroup is located at /
home/vagrant/eltex_auth_service_backup.sql
```

Creating a dump

```
Replaced role client_admindefault_1 with default_client_admin for 1 users
```

Replacing 'client_admindefault_1' with 'default_client_admin' via user settings. After that, the role is removed from the system.

## v1.14_Resetting the password to enter the Admin Panel/Portal Constructor (EN)

By default, an account with login "**admin**" and password "**password**" is used to enter the Admin Panel. If you forgot a password to the **admin** account, it can be reset to the default one. To reset your password, run the script `reset-admin-password.sh`. The script is located at the directory `/usr/lib/eltex-wifi-cab/reset-admin-password.sh`.

The script is run with the parameters `reset-admin-password.sh [<login> <password>]`, where

login - mysql account login,

password - mysql account password.

Script launch example:

```
$ cd /usr/lib/eltex-wifi-cab/
$ ./reset-admin-password.sh root q3fjc6g
Reset Wi-Fi Cab/Portal admin password - OK
```

## v1.14_PCRF (EN)


- Description
- Service management
- Configuration
  - /etc/default/eltex-pcrf
  - /etc/eltex-pcrf/eltex-pcrf.json
  - /etc/eltex-pcrf/hazelcast-cluster-network.xml


## Description

The module performs the following functions:

- Authorization and authentication of users connected via BRAS (the mechanism allows providing user service based on third-party vendors' access points).
- Accumulation of accounting for all authorization mechanisms and transferring it to a database.
- Controlling the number of Wi-Fi users' simultaneous sessions for all authorization mechanisms.
- Deauthentication of Wi-Fi users authorized via WPA-enterprise modes and BRAS.
- License control and notifying an administrator of the approaching the time limit (every day at exceeding 90%) or the session number limit (every hour at exceeding 90%).

The console is available at the following link: 'http://<ip address pcrf>:7070/pcrf'.

## Service management

| Operation | Command | Response |
|---|---|---|
| Status check | `service eltex-pcrf status` | Service is running<br>`* eltex-pcrf process is running`<br><br>• Service is waiting<br>`* eltex-pcrf process is not running` |
| Service start | `service eltex-pcrf start` | Service has been started<br>`* Starting eltex-pcrf`<br><br>The service is already running<br>`* eltex-pcrf is already running` |

| | | |
|---|---|---|
| Service stop | `service eltex-pcrf stop` | Service has been stopped successfully<br>`* Stopping eltex-pcrf`<br><br>Service has not been stopped, as it was not started<br>`* eltex-pcrf is not running` |
| Service restart | `service eltex-pcrf restart` | Service has been restarted successfully<br>`* Stopping eltex-pcrf`<br>`* Starting eltex-pcrf`<br>`* eltex-pcrf is not running`<br>`* Starting eltex-pcrf` |

## Configuration

### /etc/default/eltex-pcrf

Contains basic parameters for application launch. Default configuration example:

```
# Eltex.PCRF Server daemon parameters

# Location of java binary
JAVA=/usr/bin/java

# Initial size of Java heap
JAVA_INIT_HEAP=256m
# Maximum size of Java heap
JAVA_MAX_HEAP=512m

# To monitor via JMX - jconsole to host:port
#JMX_OPTS="-Dcom.sun.management.jmxremote \
#-Dcom.sun.management.jmxremote.port=8085 \
#-Dcom.sun.management.jmxremote.authenticate=false \
#-Dcom.sun.management.jmxremote.ssl=false \
#-Djava.rmi.server.hostname=127.0.0.1"

# Options for Java Garbage Collector
GC_OPTS="-XX:+UseParallelGC \
-XX:+PrintGCDateStamps \
-XX:+PrintGCDetails \
-XX:+UseGCLogFileRotation \
-XX:NumberOfGCLogFiles=7 \
-XX:GCLogFileSize=5M \
-Xloggc:/var/log/eltex-pcrf/gc.log"
# Without log
#GC_OPTS="-XX:+UseParallelGC"

# Additional arguments to pass to java
HEAP_DUMP_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-pcrf"

# Summary JAVA_OPTS used by daemon
JAVA_OPTS="$JMX_OPTS $GC_OPTS $HEAP_DUMP_OPTS"

# Send notification
#NOTIFICATION_ADDR="admin@mail.loc"
```

| Parameter | Description |
|---|---|
| `Location of java binary JAVA=/usr/bin/java` | Java machine location |
| `JAVA_INIT_HEAP=256m JAVA_MAX_HEAP=512m` | The amount of memory allocated for application operation |

/etc/eltex-pcrf/eltex-pcrf.json

```
{
  "auth.address" : "0.0.0.0",
  "auth.port" : 31812,
  "auth.mac.open.timeout.s" : 3600,
  "auth.mac.welcome.service" : "WELCOME",

  "acct.address" : "0.0.0.0",
  "acct.ports" : [1813, 31813],

  "lease.saver.address" : "0.0.0.0",
  "lease.saver.port" : 4381,

  "aaa.instances" : 5,
  "aaa.host" : "127.0.0.1",
  "aaa.secret" : "testing123",
  "aaa.auth.port" : 1812,
  "aaa.acct.port" : 1813,
  "aaa.rest.port" : 7080,
  "aaa.timeout" : 10,
  "aaa.attempts" : 1,

  "web.monitoring.port" : 7070,

  "cluster.enable" : false,
  "cluster.eventBusPort" : 5801,

  "radius" : {
    "url" : "jdbc:mysql://localhost/radius?
useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReconnect=tru
e",
    "user" : "javauser",
    "password" : "javapassword",
    "max_pool_size" : 16
  },

  "mongo.pcrf" : {
    "connection_string": "mongodb://localhost:27017/pcrf?
waitQueueMultiple=500&connectTimeoutMS=10000&socketTimeoutMS=0",
    "db_name": "pcrf"
  },

  "mongo.ott" : {
    "connection_string": "mongodb://localhost:27017/ott?
waitQueueMultiple=500&connectTimeoutMS=10000&socketTimeoutMS=0",
    "db_name": "ott"
  },

  "session.storage" : {
    "session.check.period.s" : 300,
    "unauth.store.time.s" : 600,
```

```
    "interval.number.expired" : 3,
    "min.interval.s" : 45,
    "default.interval.s" : 600
  },

  "bras.coa" : {
    "coa.timeout" : 10,
    "coa.attempts" : 1,
    "remote.coa.port" : 3799,
    "executor.size" : 100,
    "log.clean.period.s" : 600,
    "log.store.period" : {
      "period" : 14,
      "unit" : "D"
    }
  },

  "sql.ems" : {
    "url" : "jdbc:mysql://localhost/eltex_ems?
useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReconnect=tru
e",
    "user" : "javauser",
    "password" : "javapassword",
    "max_pool_size" : 16
  },

  "sql.wireless" : {
    "url" : "jdbc:mysql://localhost/wireless?
useUnicode=true&characterEncoding=utf8&relaxAutoCommit=true&connectTimeout=5000&autoReconnect=tru
e",
    "user" : "javauser",
    "password" : "javapassword",
    "max_pool_size" : 16
  },

  "ngw" : {
    "host" : "localhost",
    "port" : 8040
  },

  "language" : "en",

  "radius.nbi" : {
    "wdsl.url" : "http://localhost:8080/axis2/services/RadiusNbiService?wsdl",
    "username" : "admin",
    "password" : "password",
    "connection.timeout.ms" : 30000,
    "request.timeout.ms" : 120000
  },

  "tariffs.update.interval" : {
```

```
    "interval" : 1,
    "unit" : "hours"
  }

}
```

| Parameter | Description |
|---|---|
| **Authorization settings** | |
| auth.address | Server interface expecting authorization requests |
| auth.port | Server port receiving authorization requests |
| auth.mac.open.timeout.s | Default "open authorization" timeout which is used if not redefined in portal settings |
| auth.mac.welcome.service | Default welcome service which is used if not redefined in tariff settings |
| **Accounting settings** | |
| acct.address | Server interface expecting accounting |
| acct.port | Server port receiving accounting packets |
| **Settings for Wi-Fi users authorization via BRAS** | |
| aaa.instances | |
| aaa.host | Eltex.RADIUS service address |
| aaa.secret | RADIUS key |
| aaa.auth.port | The port to which authorization requests are sent |
| aaa.acct.port | The port to which accounting packets are sent |
| aaa.rest.port | The port to exchange service commands with Eltex.RADIUS |
| aaa.timeout | Response timeout |
| aaa.attempts | The number of packet sending attempts |
| **The monitoring port** | |
| web.monitoring.port | The port for console operation and monitoring |
| **Clustering** | |
| cluster.enable | Enabling clustering |
| cluster.eventBusPort | The port for data exchange with cluster nodes |
| **MySQL database connection settings ('radius', 'eltex_ems', 'wireless')** | |
| url | MySQL database connection string |
| user | The login for database connection |
| password | The password for database connection |
| max_pool_size | The maximum number of connections |

| **Mongo database connection, PCRF and OTT collection** | |
|---|---|
| `connection_string` | URL for Mongo connection |
| `db_name` | The name of the database to which the connection is made to (duplicate the content of URI) |
| **Mongo active session parameters** | |
| `session.check.period.s` | Checking period of stored sessions relevance. If a session is closed during the check period, or if its storage time is up, it will be deleted from a database. |
| `unauth.store.time.s` | Storage period of unauthorized BRAS users' sessions. |
| `interval.number.expired` | The number of missed accounting intervals, upon the exceeding of which a session is considered to be "hanging" and should be closed. |
| `min.interval.s` | The minimum accounting interval that is used to calculate hanging sessions. |
| `default.interval.s` | The default accounting interval that is saved to a session right after its creation. |
| **CoA sending parameters** | |
| `coa.timeout` | Command response timeout |
| `coa.attempts` | The number of resendings |
| `remote.coa.port` | The port to which commands will be sent |
| `executor.size` | The number of commands executed simultaneously |
| `log.store.period` | Results storage time |
| `log.store.period` | Command execution logs storage time |
| **NGW interaction parameters** | |
| `host` | Notification GW service's address |
| `port` | The port for receiving notification requests |
| **Setting a language for error messages** | |
| `language` | The language used for logging, "en" by default. "ru" value can be selected as well, but not all the logs are translated to Russian. |
| **Setting NBI service connection** | |
| `wdsl.url` | The address for NBI service requests |
| `username` | Account login |
| `password` | Account password |
| `connection.timeout.ms` | Service connection timeout |
| `request.timeout.ms` | Service request timeout |

| **Tariff update interval** | |
|---|---|
| `interval` | Tariff update interval |
| `unit` | Measurement units ("hours" by default) |

### /etc/eltex-pcrf/hazelcast-cluster-network.xml

This file contains configuration of Hazelcast cluster that is used for PCRF nodes grouping.

Example of default configuration of group and network sections (containing parameters for PCRF neighbouring nodes connection):

```
<hazelcast>

    <!-- You can separate your clusters in a simple way by specifying group names. -->
    <group>
        <name>dev</name>
    </group>

    <network>
        <!-- Write here public address of the node -->
        <public-address>192.168.0.1</public-address>
        <port auto-increment="false" port-count="100">5701</port>
        <outbound-ports>
            <ports>0</ports>
        </outbound-ports>
        <join>
            <multicast enabled="false"/>
            <tcp-ip enabled="true">
                <!-- Write here IP of all members of the cluster (including this) -->
                <member>192.168.0.1</member>
                <member>192.168.0.2</member>
            </tcp-ip>
            <discovery-strategies>
            </discovery-strategies>
        </join>
        <interfaces enabled="true">
            <!-- Write here IP of the interface to use for cluster -->
            <interface>192.168.0.1</interface>
        </interfaces>
        <ssl enabled="false"/>
        <socket-interceptor enabled="false"/>
        <symmetric-encryption enabled="false">
            <algorithm>PBEWithMD5AndDES</algorithm>
            <!-- salt value to use when generating the secret key -->
            <salt>thesalt</salt>
            <!-- pass phrase to use when generating the secret key -->
            <password>thepass</password>
            <!-- iteration count to use when generating the secret key -->
            <iteration-count>19</iteration-count>
        </symmetric-encryption>
    </network>
</hazelcast>
```

| Parameter | Description |
|---|---|
| `<name>dev</name>` | Node name (it should be the same for all devices). If nodes have different names, they are not grouped into a cluster. |
| `<public-address>192.168.0.1</public-address>` | Node's own address in a cluster. |

| | |
|---|---|
| <member>192.168.0.1</member><br><br><member>192.168.0.2</member> | The list of cluster members (specify both own address and all cluster nodes' addresses). |
| <interface>192.168.0.1</interface> | Address of node interface in a cluster (it usually equals public-address). |

## v1.14_Description of log errors

### Invalid RADIUS Authenticator

The error occurs if an access point returns invalid authenticator.
Possible causes:

- Invalid radius secret is specified on the access point
- The firmware of the access point is outdated (version 1.10.0 or lower)

Error example:

```
2017-08-31 05:25:03,654 ERROR [PcrfJsonTools:310] {
  "key" : "PcrfErrorCode.coaRequestFailed",
  "message" : "CoA request to 126.0.0.86 failed: Invalid RADIUS Authenticator",
  "code" : 15,
  "args" : [ "126.0.0.86", "Invalid RADIUS Authenticator" ]
}
net.jradius.exception.RadiusSecurityException: Invalid RADIUS Authenticator
        at net.jradius.client.RadiusClientTransport.sendReceive(RadiusClientTransport.java:123)
        at net.jradius.client.RadiusClient.sendReceive(RadiusClient.java:299)
        at org.eltex.softwlc.pcrf.vertx.radius.coa.BrasCoaHandler.run(BrasCoaHandler.java:92)
        at java.util.concurrent.CompletableFuture$AsyncRun.run(CompletableFuture.java:1626)
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
2017-08-31 05:25:03,654 ERROR [DisconnectHandler:117] Possibility of a known issue with WEP/WOP
version 1.9 generating wrong RADIUS Authenticator
```

## v1.14_Additional software (EN)


- snmpd
  - Description
  - Starting/stopping procedure
  - Configuration
- tftp-hpa
  - Description
  - Configuration

- ntpd
    - Description
    - Starting/stopping procedure
    - Configuration
- rsyslog
    - Description
    - Starting/stopping procedure
    - Configuration


SoftWLC uses additional open-source software for its work. Description and configuration parameters of each service are given below.

## snmpd

### Description

snmpd service is used for EMS servers' parameters and reservation system monitoring. The service also generates alert messages if reservation system failures occur.

### Starting/stopping procedure

snmpd server starts automatically together with the server.

To stop the service, the following command is used:

```
service snmpd stop
```

To start the service after stopping:

```
service snmpd start
```

To check the service status, use the command:

```
service snmpd status
```

This will be followed by a message:

```
* snmpd is running
```

if the service is running, or by

```
* snmpd is not running
```

if it is not.

### Configuration

snmpd service configuration file is located in **/etc/snmp/snmpd.conf** with the following contents:

**/etc/snmp/snmpd.conf**

```
# sec.name source community
#com2sec paranoid default public
com2sec readonly default public
com2sec readwrite default private
# readwrite ON for Keepalived SNMP SET support
####
# Second, map the security names into group names:
# sec.model sec.name
group MyROSystem v1 paranoid
group MyROSystem v2c paranoid
group MyROSystem usm paranoid
group MyROGroup v1 readonly
group MyROGroup v2c readonly
group MyROGroup usm readonly
group MyRWGroup v1 readwrite
group MyRWGroup v2c readwrite
group MyRWGroup usm readwrite
####
# Third, create a view for us to let the groups have rights to:
# incl/excl subtree mask
view all included .1 80
view system included .1.3.6.1.2.1.1
#view system included .iso.org.dod.internet.mgmt.mib-2.system
####
# Finally, grant the 2 groups access to the 1 view with different
# write permissions:
# context sec.model sec.level match read write notif
access MyROSystem "" any noauth exact system none none
access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all all none
syslocation Unknown (configure /etc/snmp/snmpd.conf)
syscontact Root <root@localhost> (configure /etc/snmp/snmpd.conf)
# For Keepalived SNMP support
master agentx
```

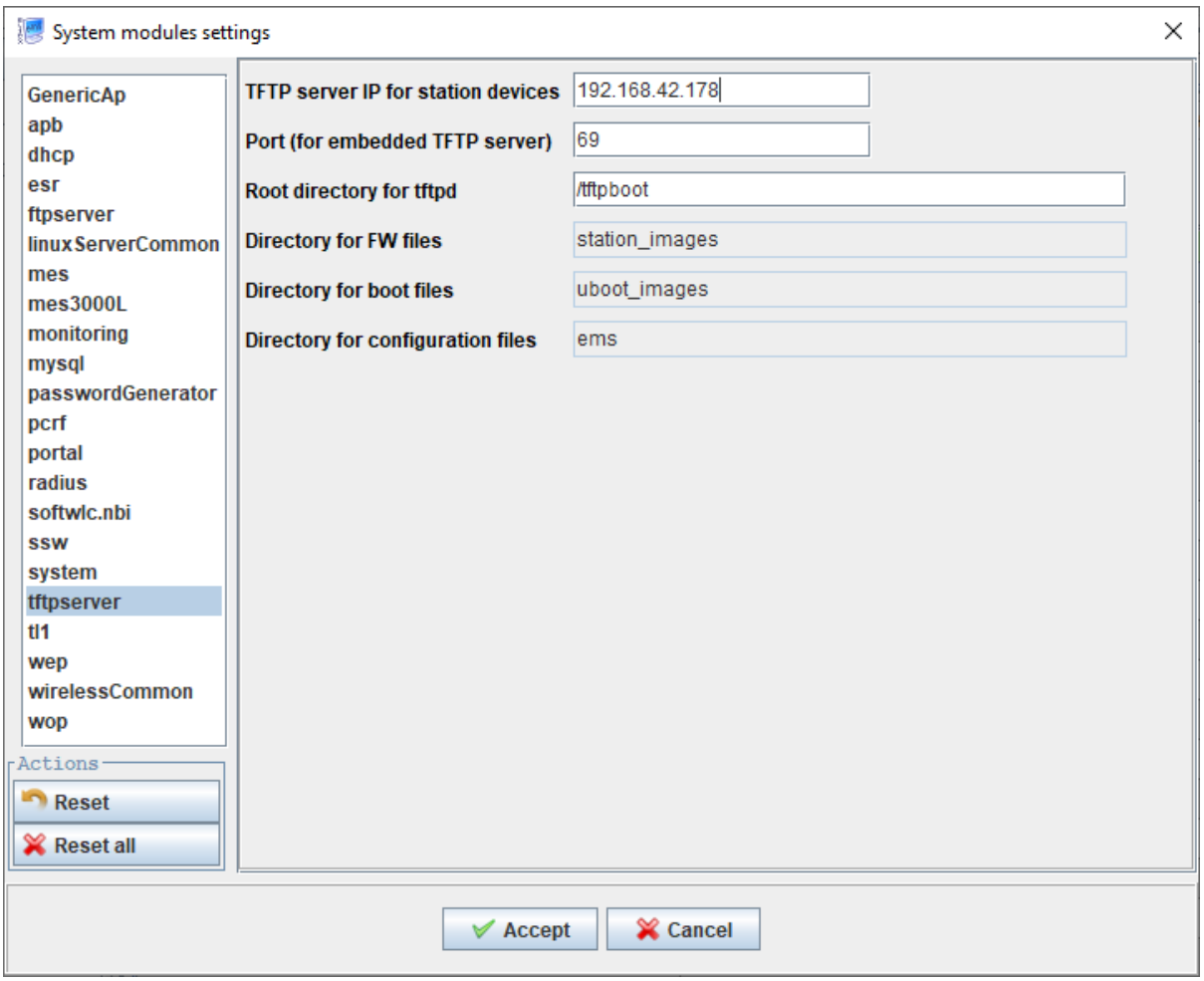
## tftp-hpa

### Description

The service is intended to update access point firmware using TFTP and to get packet-capture results from an access point.

### Configuration

The service is configured via EMS GUI. Select Administration → EMS server configuration → System modules. In the opened window, select tftpserver in the list on the left.




## ntpd

### Description

NTP — time synchronization service which is used to provide correct logging.

### Starting/stopping procedure

To stop the service, the following command is used:

```
service ntp stop
```

To start the service after stopping:

```
service ntp start
```

To check the service status, use the command:

```
service ntp status
```

This will be followed by a message:

```
* NTP server is running
```

if the service is running, or by

```
* NTP server is not running
```

if it is not.

To start synchronization manually, stop ntpd process and run the command:

```
ntpdate <your ntp server>
```

To save the current time to the hardware clock, the following command is used:

```
hwclock --systohc
```

### Configuration

***/etc/ntp.conf*** — time synchronization configuration. Specify NTP servers in the configuration file.

Example:

**Eltex.EMS Server is running with pid 1200**

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 172.17.209.9
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org
server 3.pool.ntp.org
```

In the file ***/etc/timezone*** your time zone should be specified, for example:

```
Asia/Novosibirsk
```

To configure the time zone, use the command:

```
dpkg-reconfigure tzdata
```

select your region and time zone in the opened window.

## rsyslog

### Description

The process sends syslog from the server to MySQL database.

### Starting/stopping procedure

To stop the service, the following command is used:

```
service rsyslog stop
```

To start the service after stopping:

```
service rsyslog start
```

To check the service status, use the command:

```
service rsyslog status
```

This will be followed by a message:

```
* rsyslog start/running, process 793
```

if the service is running, or by

```
* rsyslog is not running
```

if it is not.

### Configuration

Specify syslog message format and message processing rules in ***/etc/rsyslog.d/mysql.conf***:

```
### Configuration file for rsyslog-mysql
### Changes are preserved
$template StdSQLFormat,"insert into SystemEvents (Message, Facility,FromHost, FromHostIp,
Priority, DeviceReportedTime, ReceivedAt, InfoUnitID, SysLogTag) values ('%msg%',
%syslogfacility%, '%HOSTNAME%', '%fromhost-ip%', %syslogpriority%, '%timereported:::date-mysql%',
'%timegenerated:::date-mysql%', %iut%, '%syslogtag%')",SQL
$ModLoadommysql
### . :ommysql:localhost,,,
### создать правила обработки:
:fromhost-ip, !isequal, "127.0.0.1" :ommysql:172.17.209.6,Syslog,rsyslog,root; StdSQLFormat
```

where **StdSQLFormat** – the format for transferring syslog from access points to the database;

**172.17.209.6** – database IP address.

Allow receiving messages from access points in **/etc/rsyslog.conf** by uncommenting the following lines:

```
provides UDP syslog reception
$ModLoadimudp
$UDPServerRun 514
provides TCP syslog reception
$ModLoadimtcp
$InputTCPServerRun 514
```

## v1.14_NGINX for single-host installations

Due to creating a separate servlet for eltex-portal service, problems may occur for single-host installations. This is related to the necessity of network reconfiguration for keeping the portal authorization service in working condition. One of the possible solutions is to start a nginx-based proxy server to provide communication via port 8080 "as before".
In this section nginx installation and configuration instructions are given. Necessary changes that should be introduced to tomcat configuration are noted too.

### NGINX installation and configuration

NGINX v1.12.2 or higher is required. Detailed installation instructions can be found on the official website: https://nginx.ru/en/linux_packages.html#stable
After installation, add softwlc.conf configuration file to **/etc/nginx/conf.d/** directory.

### tomcat configuration

open the configuration file
`/etc/tomcat7/server.xml`

and change the listened port from 8080 to 8081 in **Service** section:

```
    <Connector port="8081" protocol="HTTP/1.1"
               connectionTimeout="20000"
               URIEncoding="UTF-8"
               redirectPort="8443" />
```

add header proxying in **Host** section:

```
<Valve className="org.apache.catalina.valves.RemoteIpValve"
   remoteIpHeader="X-Forwarded-For"
   internalProxies="127\.0\.0\.1"
   requestAttributesEnabled="true"/>
```

The example of final configuration (commented-out lines are deleted): server.xml

After changing configuration files, restart tomcat to release port 8080 and then nginx to start proxying. All web servers will continue working as before.

## v1.14_Authentication and authorization in MongoDB

### Congifuring authentication in a cluster

For cluster nodes authentication, create a file with the key of 6-1024 Base64 symbols. That can be done in the following way:

```
openssl rand -base64 741 > mongo_keyfile
```

This file should have numerical permission 400, so allow owner to read the file and define ownership.

```
chown mongodb mongo_keyfile
chmod 400 mongo_keyfile
```

After that, add `keyfile` parameter containing an absolute path to the created file to `/etc/mongodb.conf` (in the example considered, add keyFile = /etc/mongo_keyfile line) and restart MongoDB.

This should be done for each node of the cluster:

Copy the file to each node of the cluster, check permissions and file owner.

**Specification of keyFile automatically enables authentication (`auth = true`).**

Then user configuration should be performed.

### User configuration

#### Creating administrator account

To create administrator account using Mongo shell, the following will need to be done:

1) Connect to admin database:

```
$ mongo admin
connecting to: admin
>
```

2) Enter the command to create a user

```
db.addUser({ user: "<username>", pwd: "<password>", roles: [ "clusterAdmin",
"userAdminAnyDatabase", "dbAdminAnyDatabase", "readWriteAnyDatabase" ] })
```

After administrator account has been created, restart MongoDB service. If authentication was not configured in the cluster, set auth = true in /etc/mongodb.conf  configuration file

```
service mongodb restart
```

After service restart, mongo can be accessible using the new user account.

```
mongo -u<username> -p<password> admin
```

admin is the name of the database to which connection is made.

Then users for other databases should be added. In particular for DB: notification-gw, pcrf, wifi-customer-cab

Regular users are added in the same way as administrator, but with readWrite (reading/writing) and dbAdmin (some operations with indices and collections) roles:

Select the required database

```
> use  notification-gw
```

Create a user

```
> db.addUser(\{ user: "<user_name>", pwd: "<password>", roles: \[ "readWrite", "dbAdmin" \] \})
```

Switch to another database

```
> use   pcrf
```

Repeat the operation for PCRF using the same privileges, but add clusterAdmin privilege to get replica set state.

```
> db.addUser(\{ user: "<user_name>", pwd: "<password>", roles: \[ "readWrite", "dbAdmin",
clusterAdmin \] \})
```

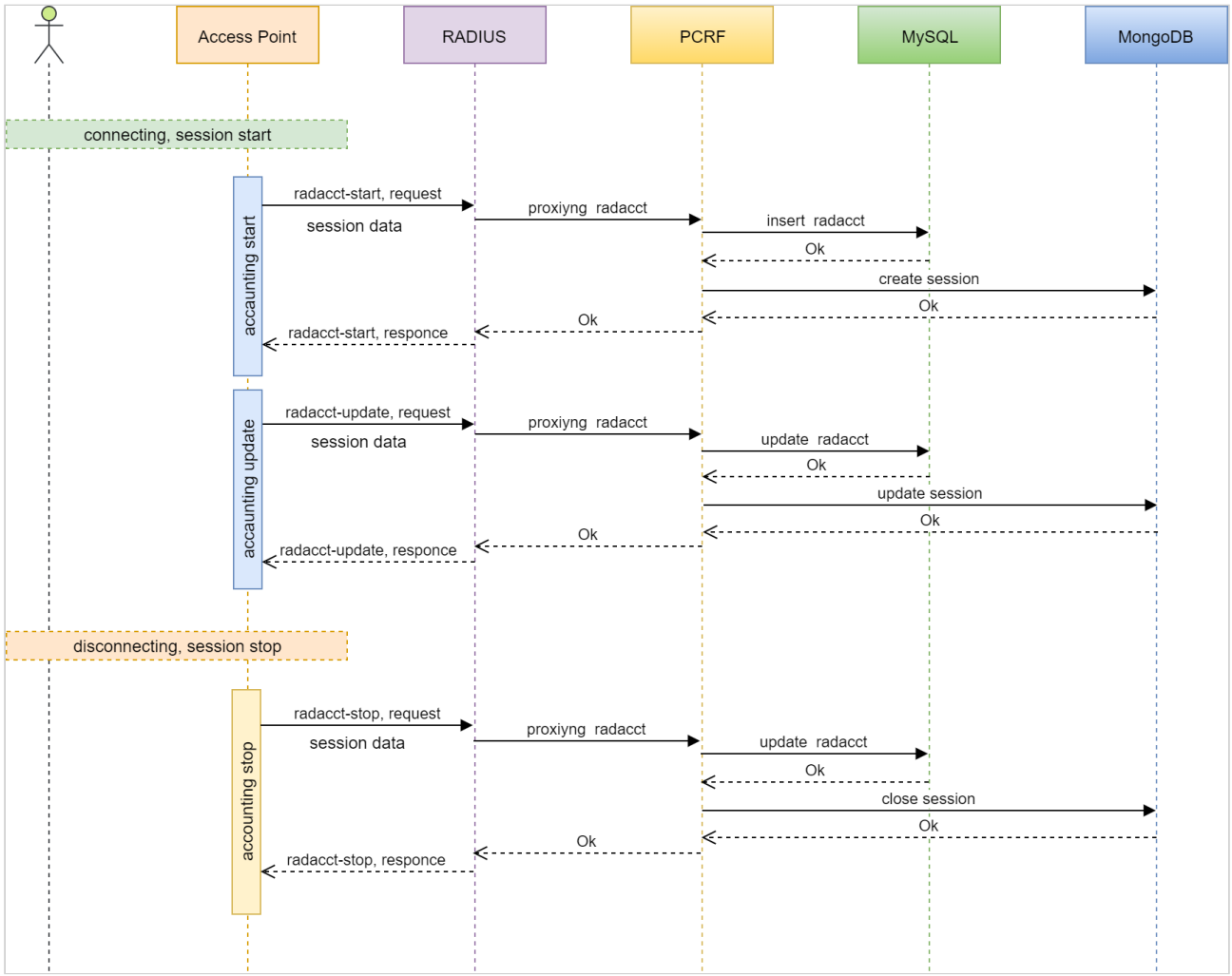
Do not forget to specify login and password for `wifi-customer-cab` database access in `/etc/eltex-wifi-cab/system.xml` configuration file of Admin Panel.

Configure pcrf access in `/etc/eltex-radius-nbi/radius_nbi_config.txt`.

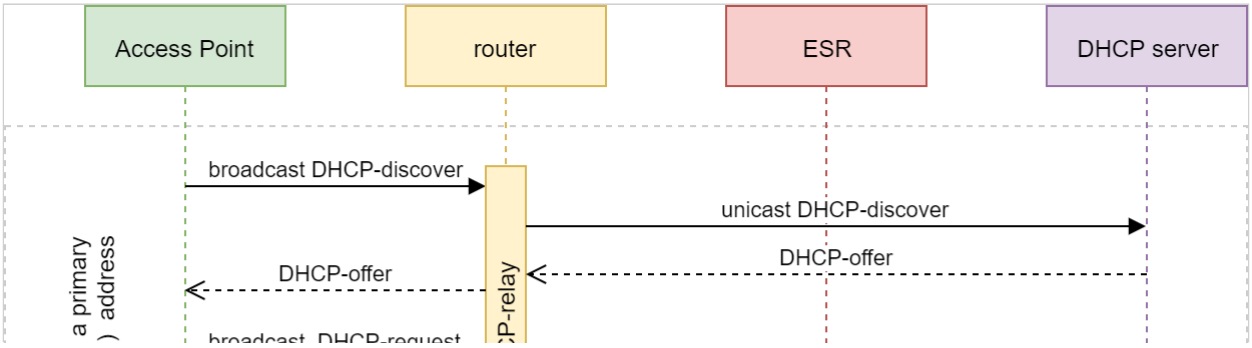
Configure `notification-gw access` in `/etc/eltex-notification-gw/notification.properties`.

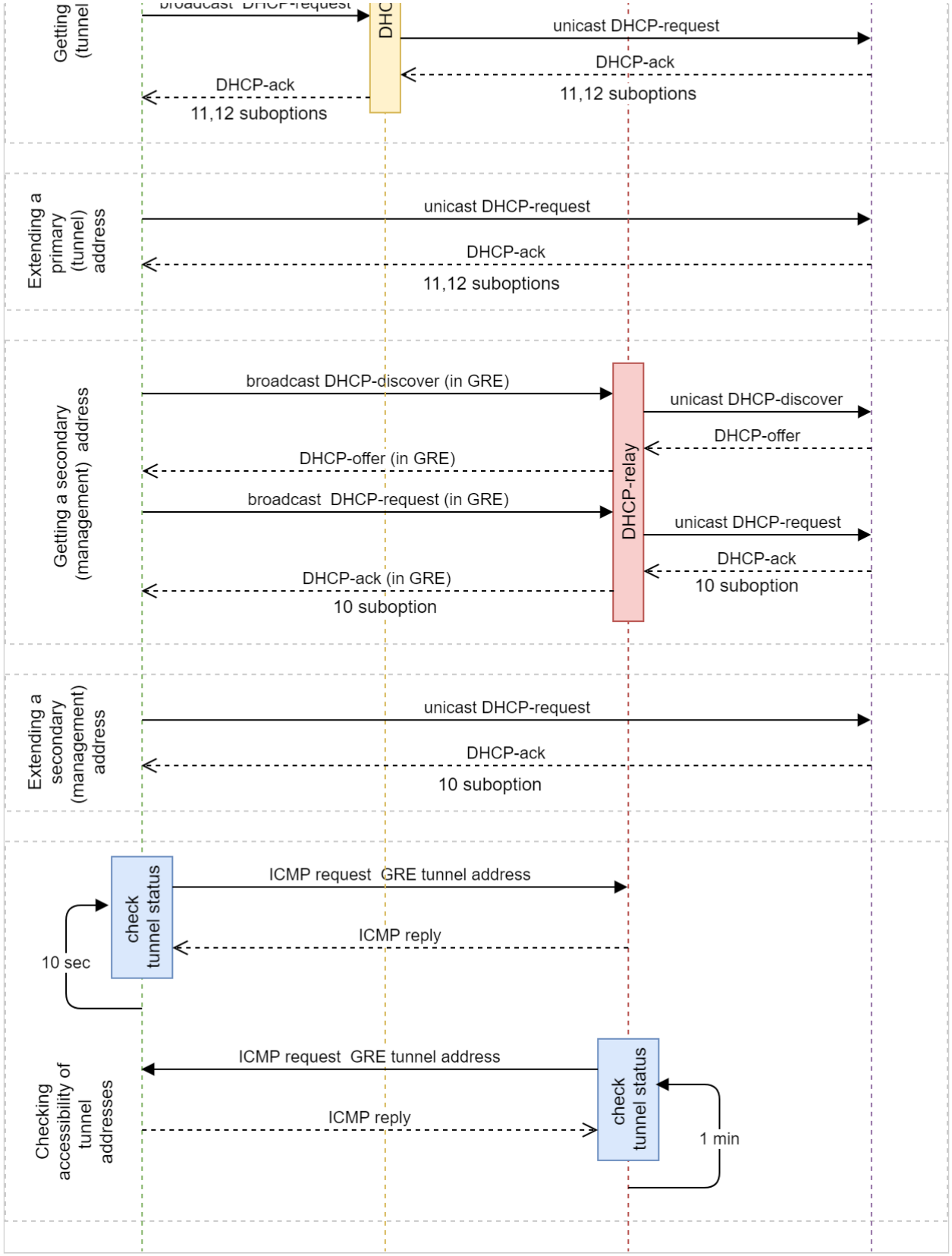
# v1.14_Schemes and algorithms (EN)

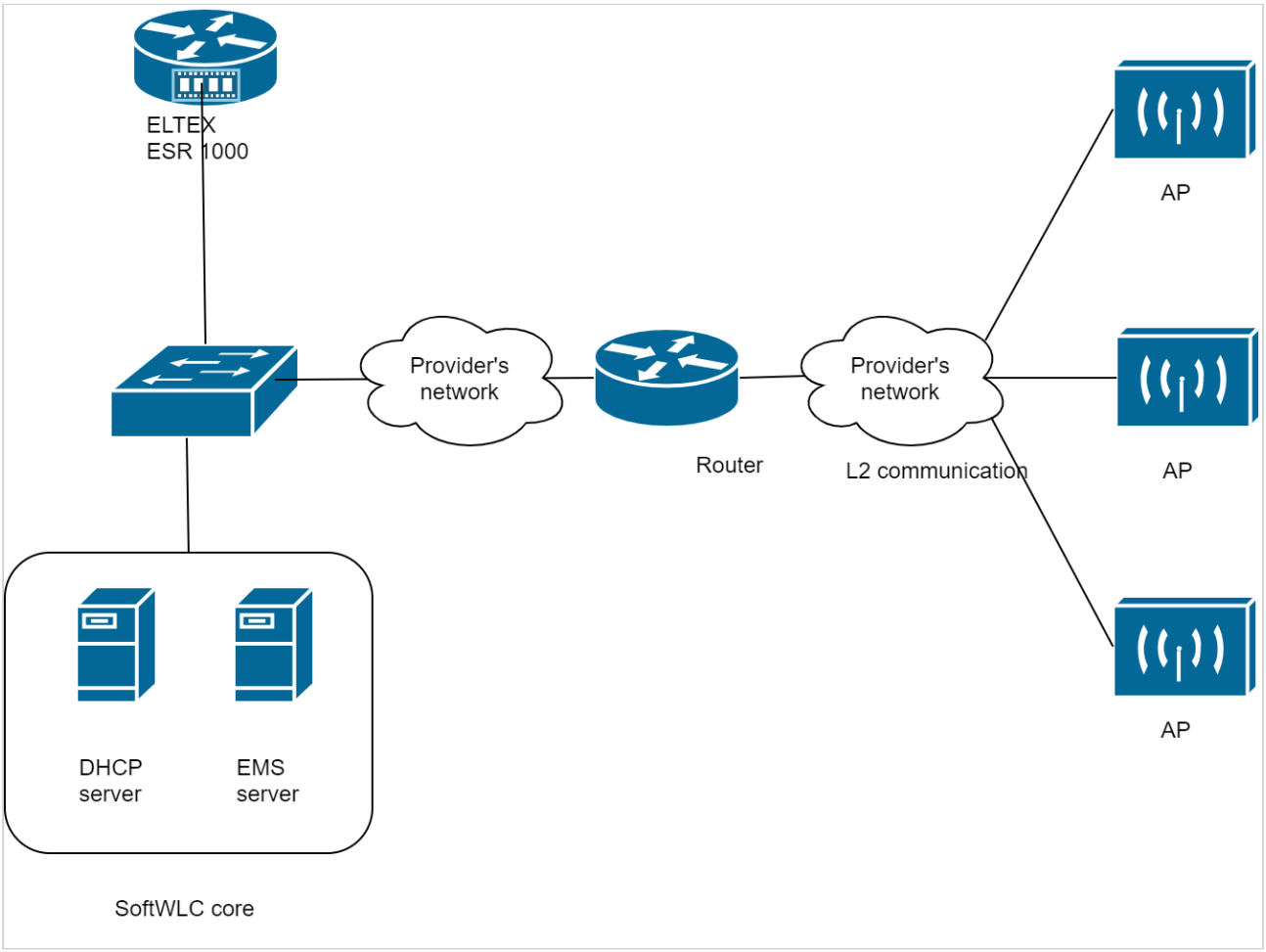
## v1.14_Algorithm for accounting processing



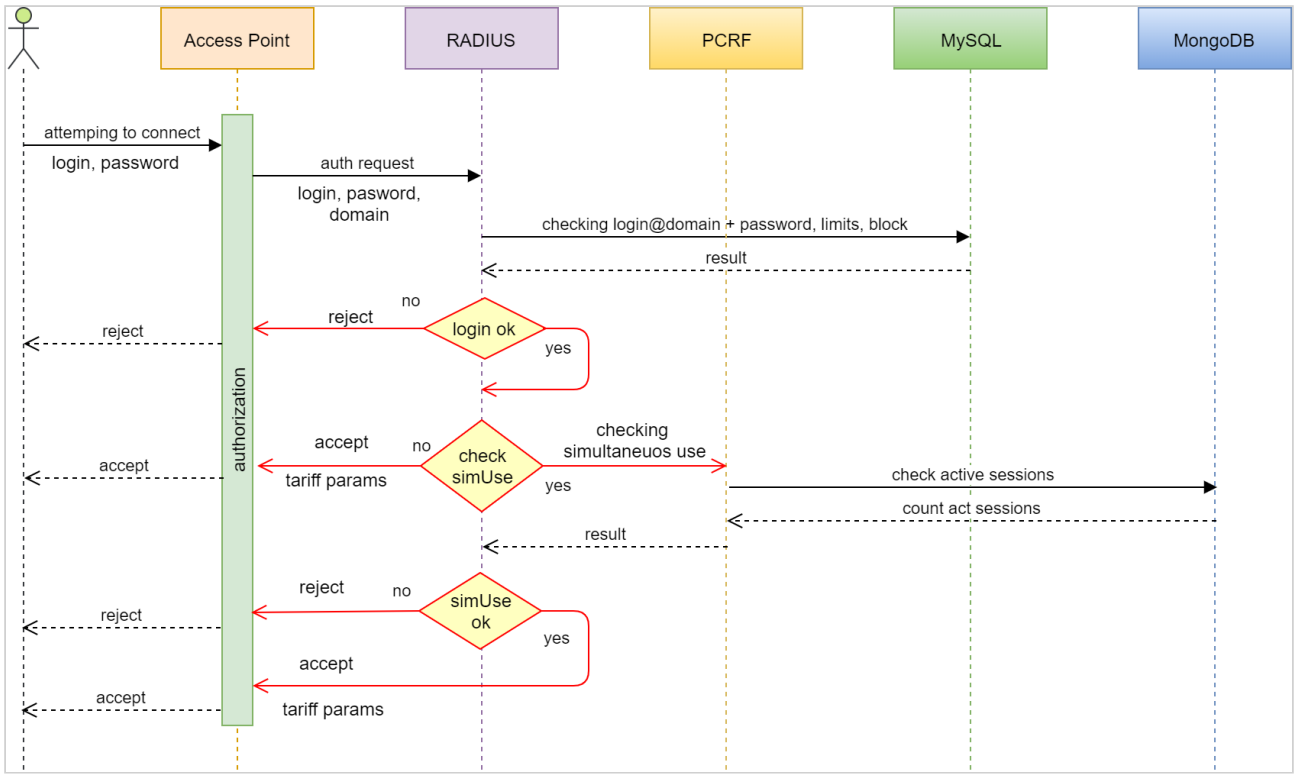

## v1.14_Algorithm for establishing GRE tunnels and getting IP addresses by access points

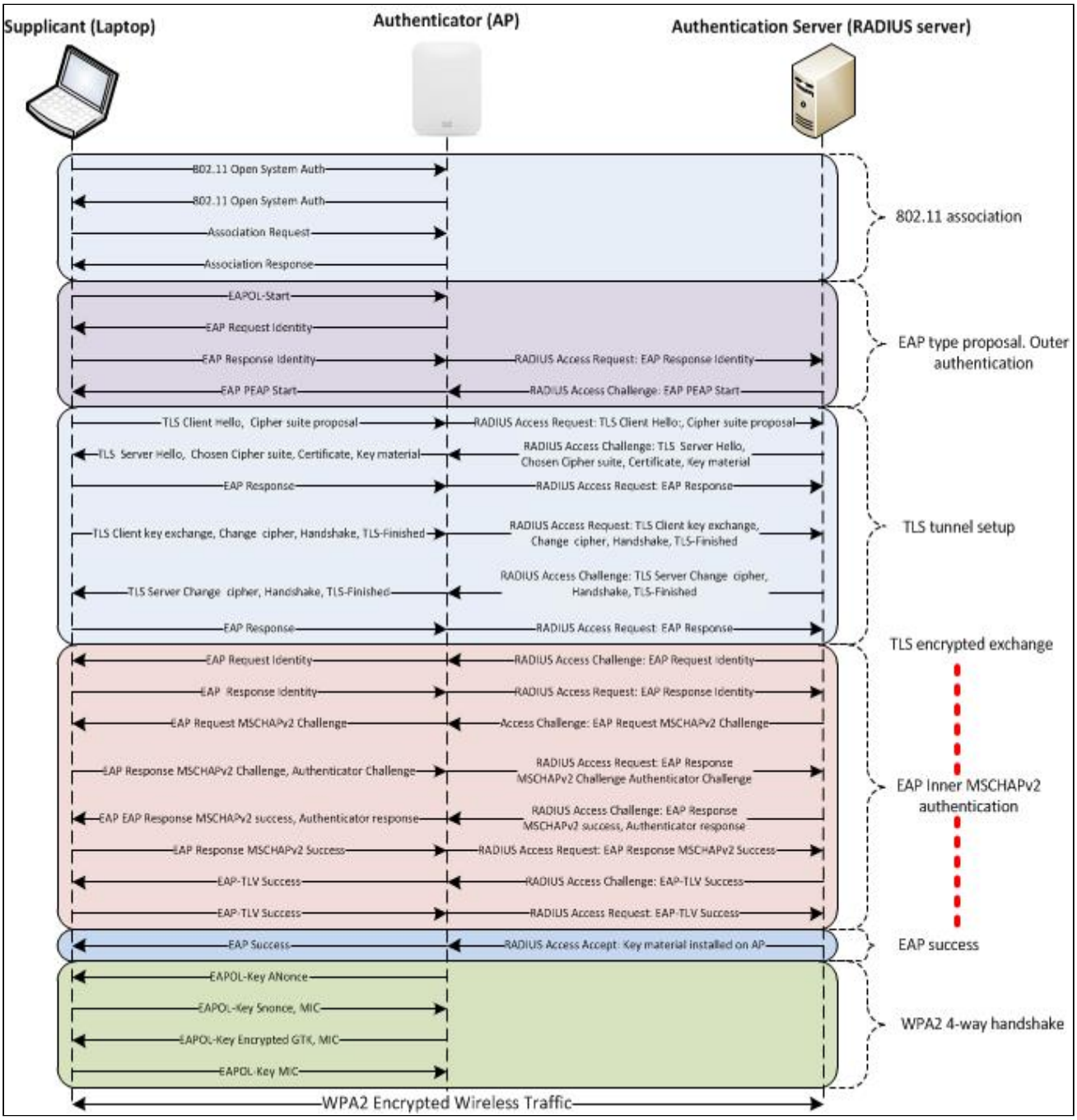



Getting (tunnel
DHC
unicast DHCP-request
DHCP-ack
11,12 suboptions
DHCP-ack
11,12 suboptions
Extending a primary (tunnel) address
unicast DHCP-request
DHCP-ack
11,12 suboptions
Getting a secondary (management) address
broadcast DHCP-discover (in GRE)
unicast DHCP-discover
DHCP-offer
DHCP-offer (in GRE)
broadcast DHCP-request (in GRE)
unicast DHCP-request
DHCP-ack
10 suboption
DHCP-ack (in GRE)
10 suboption
DHCP-relay
Extending a secondary (management) address
unicast DHCP-request
DHCP-ack
10 suboption
check tunnel status
ICMP request GRE tunnel address
ICMP reply
10 sec
Checking accessibility of tunnel addresses
ICMP request GRE tunnel address
ICMP reply
check tunnel status
1 min

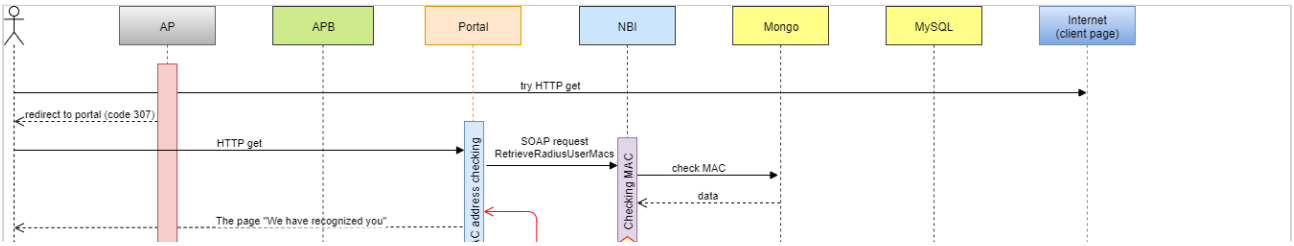

ELTEX
ESR 1000
Provider's
network
Router
Provider's
network
L2 communication
AP
AP
AP
DHCP
server
EMS
server
SoftWLC core

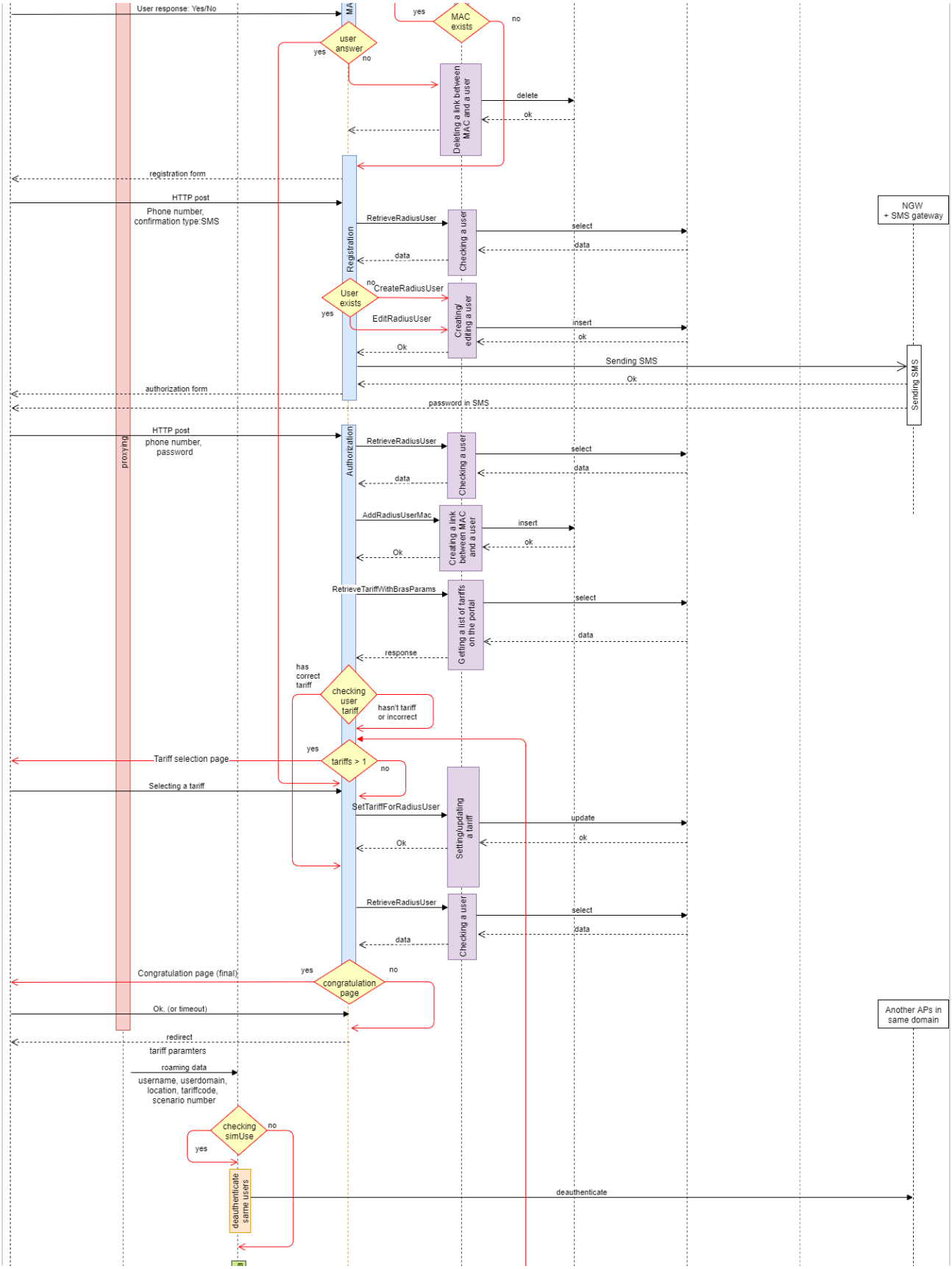
# v1.14_Algorithm for working with enterprise users on Eltex access points

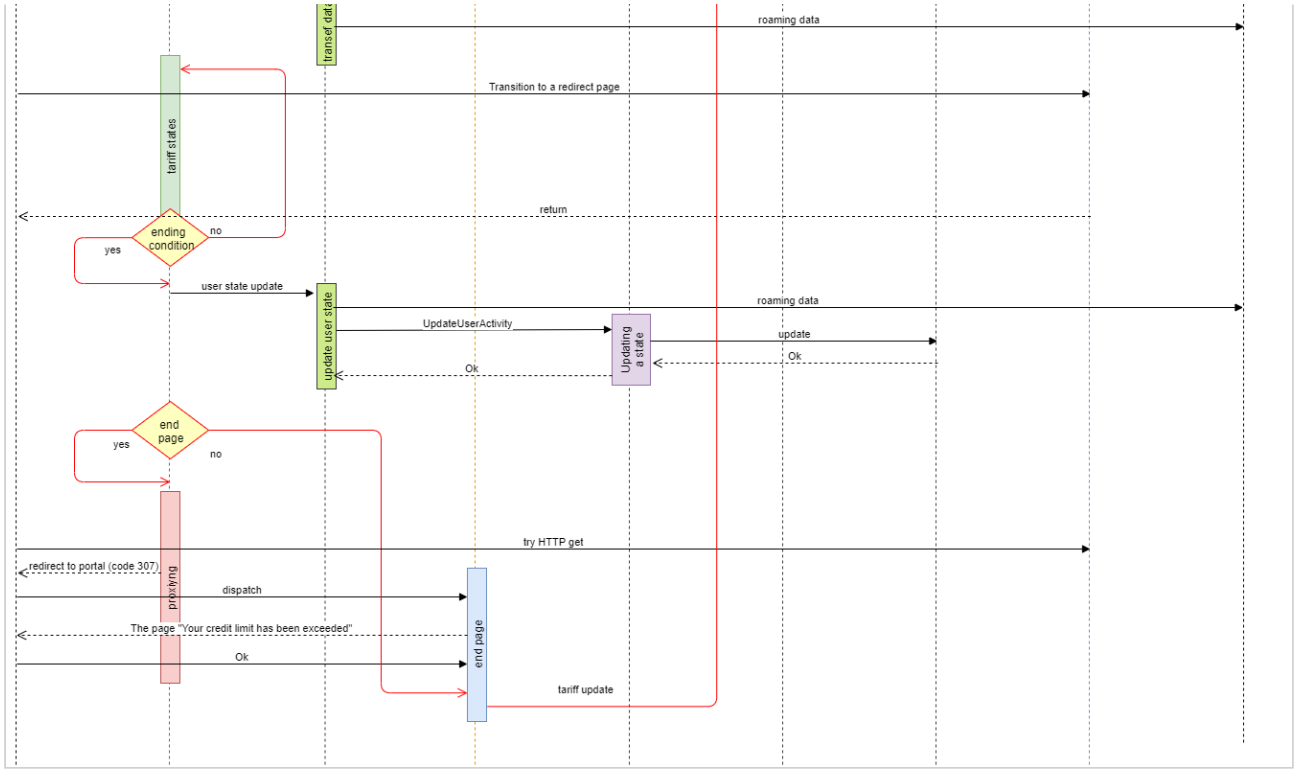




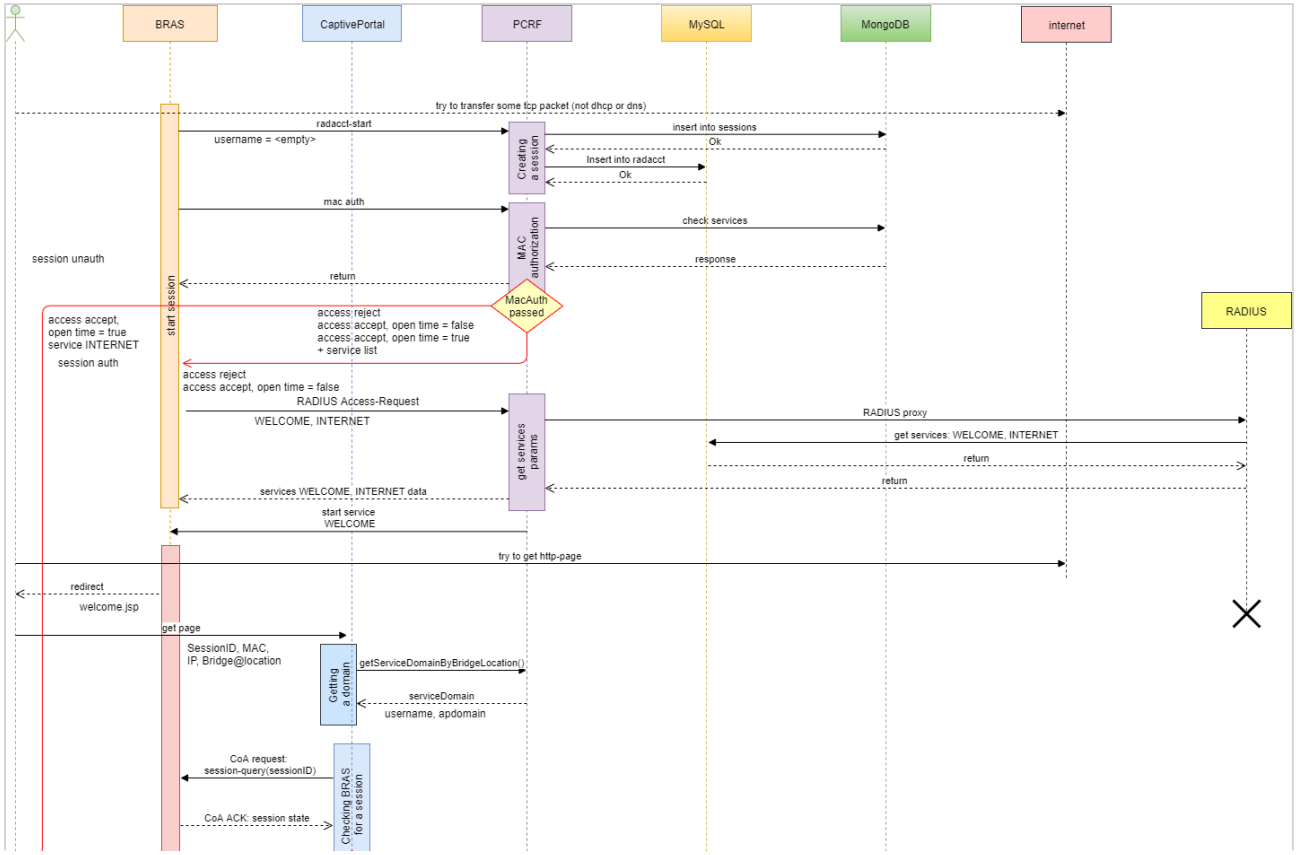

## v1.14_Algorithm for working with portal users on Eltex access points

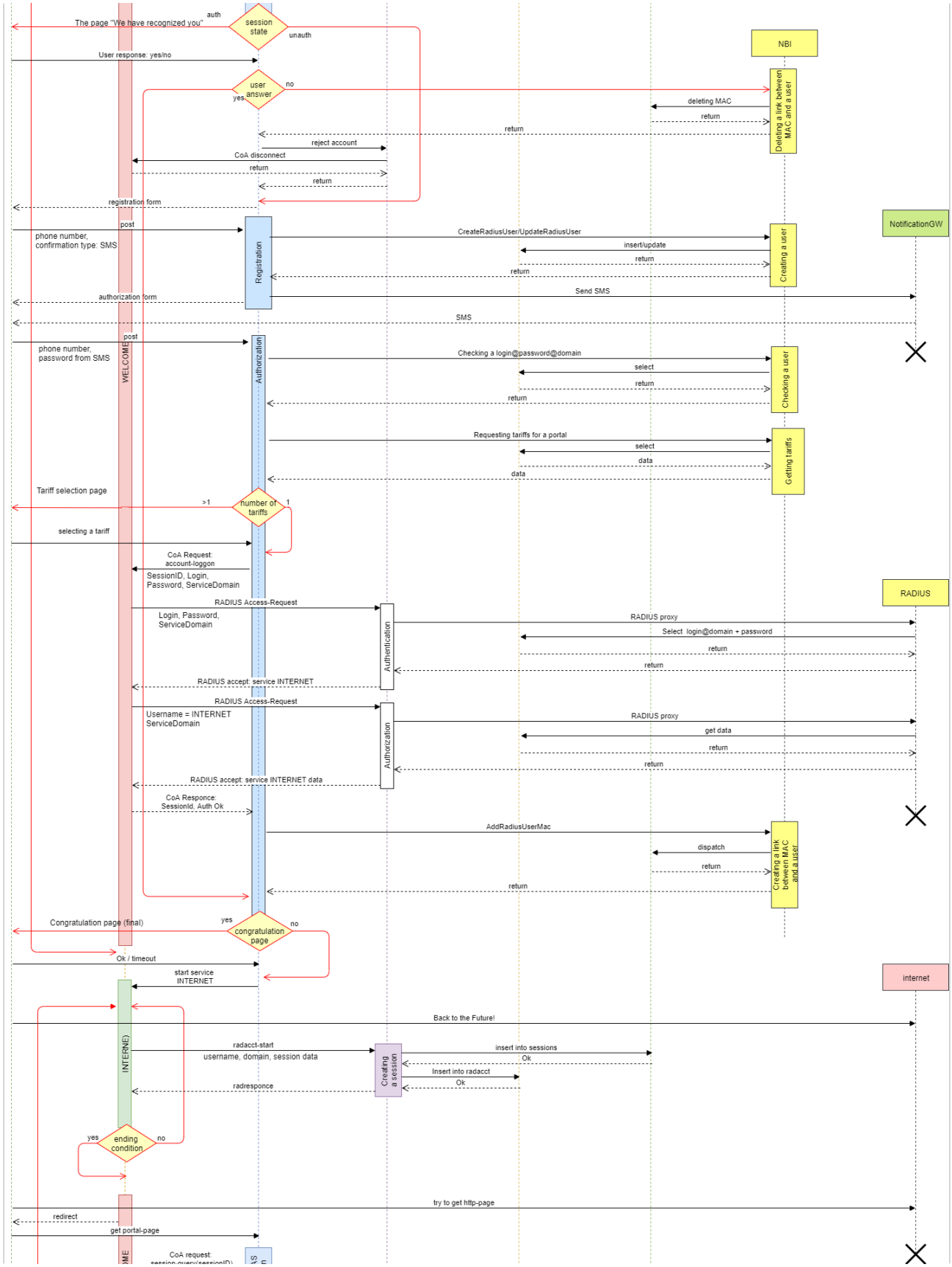


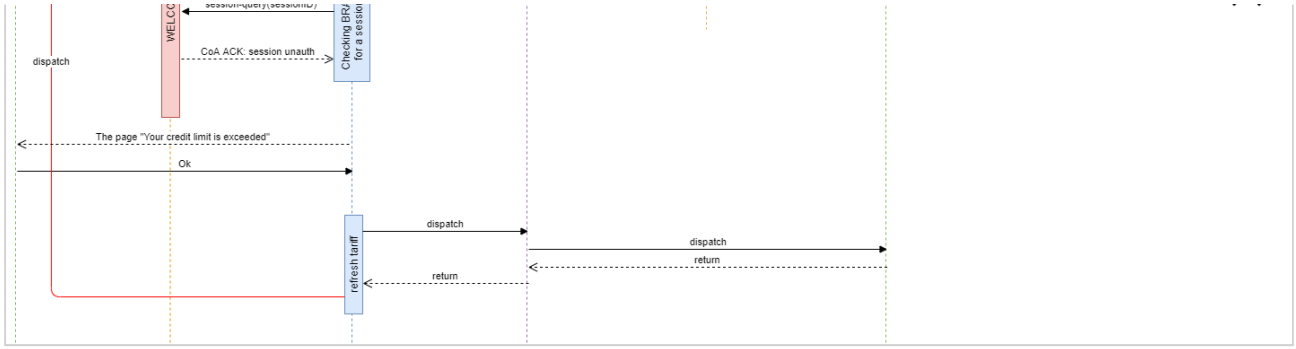

User response: Yes/No
MAC exists
yes
no
user answer
yes
no
Deleting a link between MAC and a user
delete
ok
registration form
HTTP post
Phone number, confirmation type:SMS
Registration
RetrieveRadiusUser
Checking a user
select
data
NGW + SMS gateway
User exists
no
yes
CreateRadiusUser
EditRadiusUser
Creating/ editing a user
insert
ok
Ok
Sending SMS
Ok
Sending SMS
authorization form
password in SMS
HTTP post
phone number, password
proxyrad
Authorization
RetrieveRadiusUser
Checking a user
select
data
AddRadiusUserMac
Creating a link between MAC and a user
insert
ok
Ok
RetrieveTariffWithBrasParams
Getting a list of tariffs on the portal
select
data
response
has correct tariff
checking user tariff
hasn't tariff or incorrect
yes
Tariff selection page
tariffs > 1
no
Selecting a tariff
SetTariffForRadiusUser
Setting/updating a tariff
update
ok
Ok
RetrieveRadiusUser
Checking a user
select
data
Congratulation page (final)
yes
congratulation page
no
Ok, (or timeout)
Another APs in same domain
redirect
tariff paramters
roaming data
username, userdomain, location, tariffcode, scenario number
checking simUse
no
yes
deauthenticate same users
deauthenticate




## v1.14_Algorithm for working with portal users when connecting via BRAS+PCRF

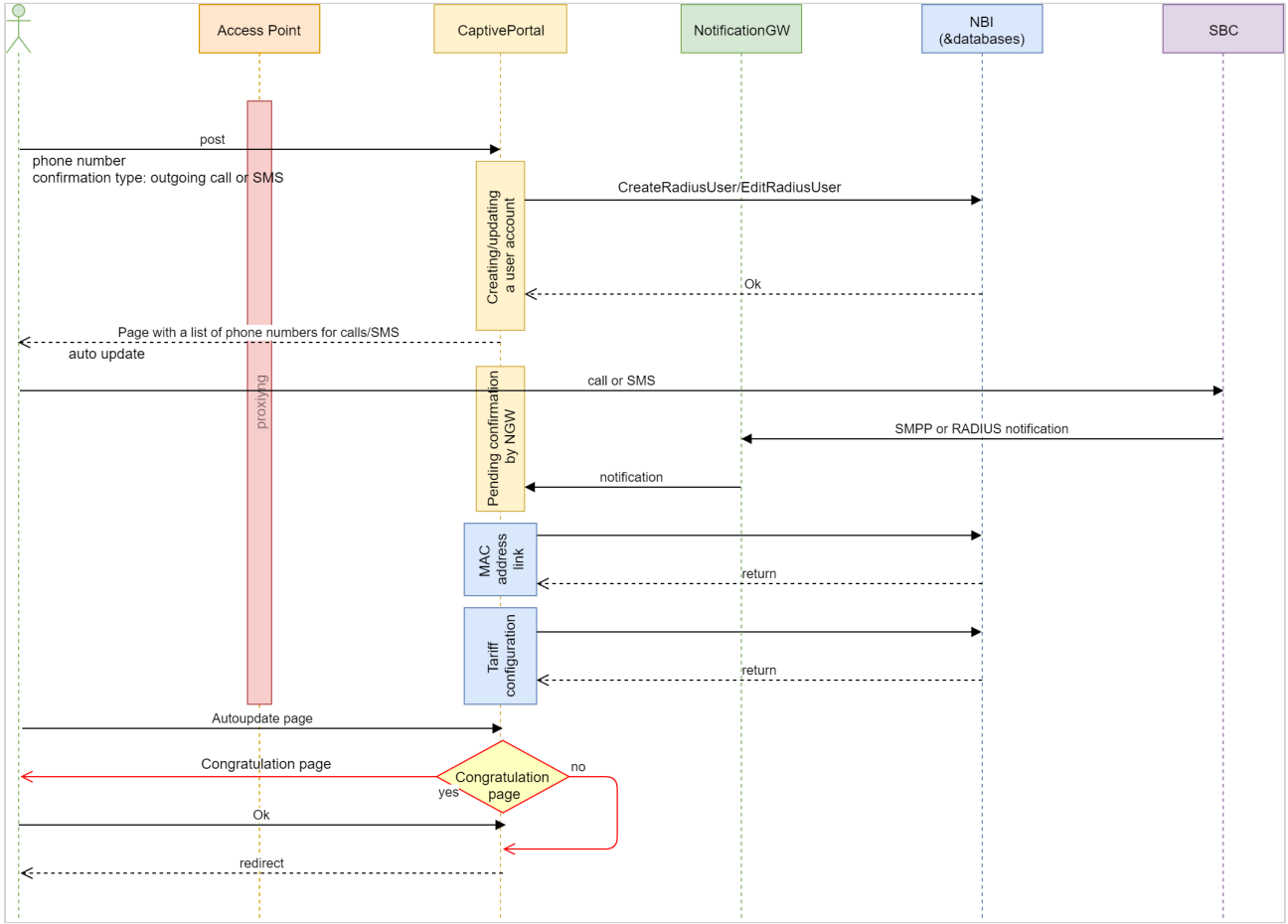



auth
The page "We have recognized you"
session state
unauth
User response: yes/no
user answer
yes
no
NBI
deleting MAC
return
Deleting a link between MAC and a user
return
reject account
CoA disconnect
return
return
registration form
post
phone number, confirmation type: SMS
Registration
CreateRadiusUser/UpdateRadiusUser
insert/update
return
return
Creating a user
NotificationGW
authorization form
Send SMS
SMS
post
phone number, password from SMS
WELCOME
Authorization
Checking a login@password@domain
select
return
return
Checking a user
Requesting tariffs for a portal
select
data
data
Getting tariffs
Tariff selection page
>1
number of tariffs
1
selecting a tariff
CoA Request: account-loggon
SessionID, Login, Password, ServiceDomain
RADIUS
RADIUS Access-Request
Login, Password, ServiceDomain
Authentication
RADIUS proxy
Select login@domain + password
return
return
RADIUS accept: service INTERNET
RADIUS Access-Request
Username = INTERNET ServiceDomain
Authorization
RADIUS proxy
get data
return
return
RADIUS accept: service INTERNET data
CoA Responce: SessionId, Auth Ok
AddRadiusUserMac
dispatch
return
return
Creating a link between MAC and a user
Congratulation page (final)
yes
congratulation page
no
Ok / timeout
start service INTERNET
internet
Back to the Future!
INTERNET)
radacct-start
username, domain, session data
Creating a session
insert into sessions
Ok
Insert into radacct
Ok
radresponce
yes
ending condition
no
try to get http-page
redirect
get portal-page
CoA request:




## v1.14_Authorization on the portal

### Account confirmation by an outgoing call or SMS




## v1.14_List of service ports

**Notation keys**

- CLI - command line interface
- GUI - graphical user interface of EMS management system

- AP - access point
- Portal - Eltex-Portal host
- APB - Eltex-APB host
- EMS - Eltex-EMS host
- PCRF - Eltex-PCRF host
- ЛК - Admin Panel host

**The ports used for SoftWLC operation:**

| Source address | Source port | Destination address | Destination port | Transport protocol | Comment |
|---|---|---|---|---|---|
| Remote access to devices from a server | | | | | |
| Server | any | Access point management network | 22 | TCP | Remote access to AP CLI via SSH |
| Server | any | Access point management network | 23 | TCP | Remote access to AP CLI via Telnet |
| Assigning IP addresses via DHCP | | | | | |
| Access point management network/Client network | 68 | DHCP server | 67 | UDP | DHCP server requests from APs and clients |
| DHCP server | 67 | Access point management network/Client network | 68 | UDP | DHCP server responses to APs and clients |
| Updating firmware on devices | | | | | |
| Access point management network | any | TFTP server | 69 | UDP | AP firmware updating via TFTP; TFTPprotocol inspection is required for data transmission |
| Transport network | any | FTP server | 21 | TCP | ESR firmware updating via FTP; FTP protocol inspection is required for data transmission |
| FTP server | any | Transport network | any | TCP | ESR firmware updating via FTP in passive mode; FTP protocol inspection is required |
| Access point management network | any | EMS server | 8080 | TCP | AP firmware updating via HTTP |
| AP monitoring and management via SNMP | | | | | |

| Source address | Source port | Destination address | Destination port | Transport protocol | Comment |
|---|---|---|---|---|---|
| EMS server | any | Access point management network | 161 | UDP/TCP | AP monitoring and management via SNMP |
| EMS server | any | Transport network | 161 | UDP | ESR/MES monitoring and management via SNMP |
| Access point management network | any | EMS server | 162 | UDP | Sending SNMP traps to the EMS server |
| Access point management network | any | EMS server | 514 | UDP/TCP | Syslog sending |
| Working with RADIUS | | | | | |
| Access point management network | any | RADIUS server | 1812 | UDP | Authentication and authorization on APs |
| Access point management network | any | RADIUS server | 1813 | UDP | RADIUS accounting |
| PCRF | any | Access point management network | 3799 | UDP | The port for CoA message exchange |
| Working with Eltex-Portal | | | | | |
| Access point management network | any | Portal | 8080 | TCP | Interaction with Eltex-Portal |
| Working with Eltex-APB | | | | | |
| Access point management network | any | APB | 8090 | TCP | Interaction with Eltex-APB |
| Working with ESR BRAS | | | | | |
| PCRF | any | ESR | 3799 | UDP | The port for CoA message exchange |
| PCRF | any | ESR | 31812 | UDP | RADIUS authentication and authorization |
| PCRF | any | ESR | 31813 | UDP | RADIUS accounting |
| ESR | any | PCRF | 7070 | UDP | PCRF API |
| ESR | any | Portal | 8080 | TCP | Interaction with Eltex-Portal |

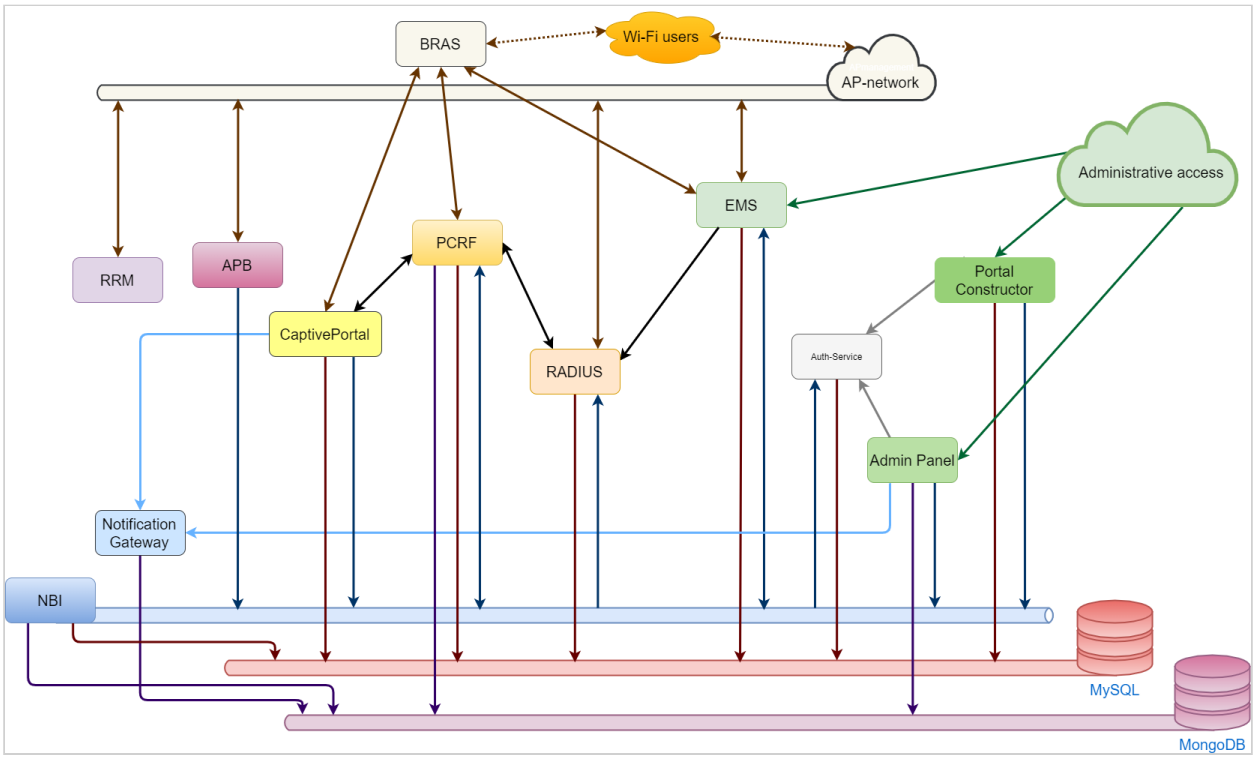
**Ports used for remote access to SoftWLC services:**

| Source address | Source port | Destination address | Destination port | Transport protocol | Comment |
|---|---|---|---|---|---|
| Remote access to a server | | | | | |

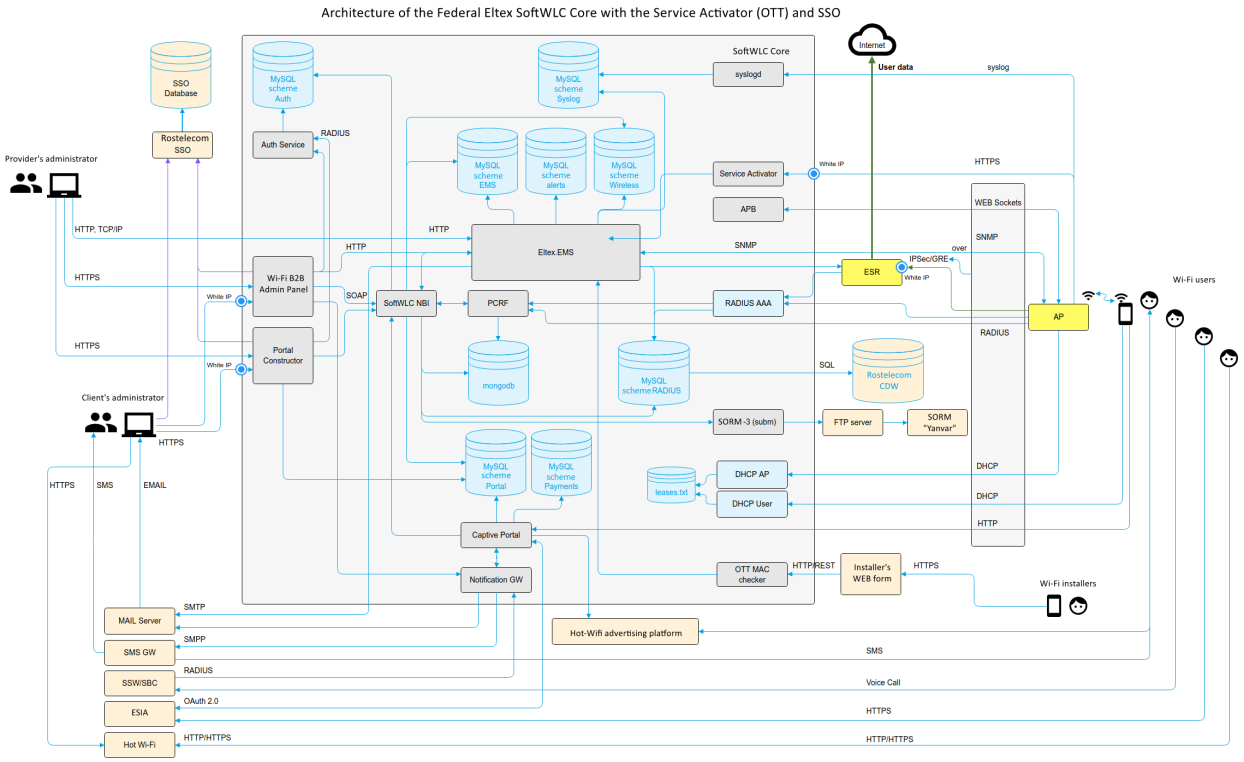
| Source address | Source port | Destination address | Destination port | Transport protocol | Comment |
|---|---|---|---|---|---|
| Administrator network | any | Server | 22 | TCP | Remote access to a server's terminal via SSH |
| Remote access to Eltex services | | | | | |
| Administrator network/Operator network | any | EMS/Admin Panel/Portal Constructor | 8080 | TCP | Access to the services: EMS, Admin Panel and Portal Constructor |
| Administrator network/Operator network | any | APB | 8090 | TCP | Access to the service APB |
| Administrator network/Operator network | any | EMS/Admin Panel/Portal Constructor | 9310 | TCP | Interaction between the applet (GUI) EMS and a server |
| Administrator network/Operator network | any | EMS/Admin Panel/Portal Constructor | 9311 | TCP | Additional port for interaction between the applet (GUI) EMS and a server, used for device CLI emulation |

## v1.14_Interaction scheme of SoftWLC components

### Simplified diagram




### Detailed diagram




## v1.14_Interaction scheme for call back authorization

| |
|---|

## v1.14_Portal Constructor (EN)


- Description
- Starting/stopping procedure
- Configuration
  - /etc/eltex-portal-constructor/application.conf
  - System settings in GUI
    - Portal Constructor
    - Alert settings
      - Notification types
        - SNMP
        - E-mail
        - SMS
    - NBI access
    - NGW access
    - BRAS access
    - Payments DB
    - PCRF access
    - Mercury access
    - Wi-Fi Customer Cab (Admin Panel)

        - ESIA login
        - SATS integration
- Gallery
    - Adding/updating images
    - Deleting images
- Dashboard
- Customer Cab
- Portals
    - Creating a new portal
    - Copying a portal
    - Common settings
        - SMS settings
        - Security settings
    - Language settings
    - Scheduler settings
        - Expanded schedule
    - Payment service
    - Tariffs
    - Appearance
        - Language
        - Preview
            - Configuring elements
        - Configuration tools
            - Colour settings
            - Selecting an image
            - Sections
                - Common
                - Configuring banners
                - Text
                - Fields
                - Buttons
        - Additional CSS


## Description

The WEB portal is included into the SoftWLC project to implement the Hotspot clients authorization model. An unknown user can connect to an access point without getting a login and a password in advance. But if he or she tries to access the Internet via a browser, he will be redirected to a WEB portal page where authorization or credentials obtaining (for example, via SMS) can be performed. During authorization, a user can see advertisement banners customized in accordance with a provider's requirements.

To customize a WEB portal, the Portal Constructor is available in SoftWLC. The Portal Constructor allows users to configure scenarios and appearance of portals used during Hotspot authorization. Users of the Portal Constructor can create and delete portals, select their background and content (text, images), set different modes and authorization scenarios for each portal. The Portal Constructor itself does not perform any actions in the service supply chain. This tool serves only for configuration.

The Portal Constructor GUI is available at the following URL: ***http://<Portal Constructor IP address>:8080/epadmin***

Login and password for the portal configuration access are specified during running its installation package. User accounts and access rights management is performed via the "Wi-Fi B2B Admin Panel".

The Portal Constructor allows configuring portals to work both with Eltex access points and BRAS (ESR-1000) that is used to connect other vendors' access points to the Platform. If BRAS is used, it should be configured in the sections "BRAS access" and "PCRF access" of the Portal Constructor.

Use the package **eltex-portal-constructor** for installation.

## Starting/stopping procedure

The interface works under tomcat (version 6 and higher), so no specific commands are needed.

## Configuration

### /etc/eltex-portal-constructor/application.conf

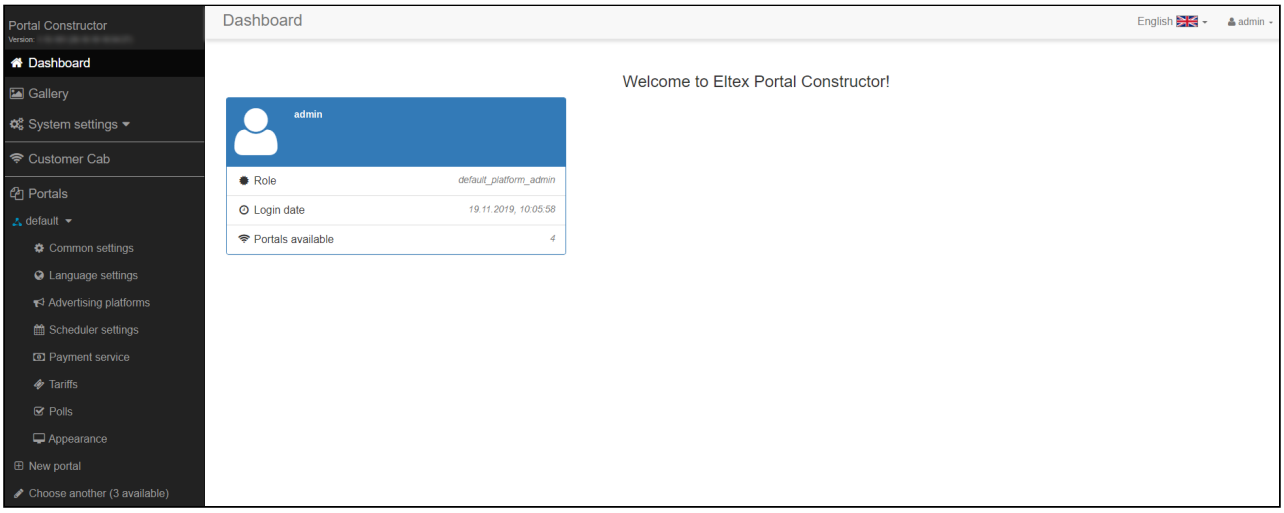
the main configuration file. Default configuration example:

```
auth-service {
    host = localhost
    port = 21812
    timeout = 10s
    retries = 3
    secret = eltex
    # pap, chap, mschapv2
    protocol = pap
}

login {
    # The number of attempts to log into Admin Panel before blocking
    maxAttemptsLogin = 3
    maxAttemptsIP = 5
    # Duration of the blocking period (in minutes) that starts after reaching the maximum number
of attempts to log into the Admin Panel
    blockTime = 5m
}

database {
    host = localhost
    port = 3306
    name = ELTEX_PORTAL
    user = javauser
    password = javapassword

    pool {
        # Time to wait for a connection
        connectionTimeout = 10s
        # Time to wait for connection validation
        validationTimeout = 3s

        min = 1
        max = 10
    }

    cache {
        # Limit of cached simple entries count (for each query type)
        maxEntries = 1000
        # Limit of total cached portal resources size
        maxResourceBytes = 32m
        # Maximum time to retain items in the cache
        expireTime = 30s
    }
}
```

| Parameter | Description |
|---|---|

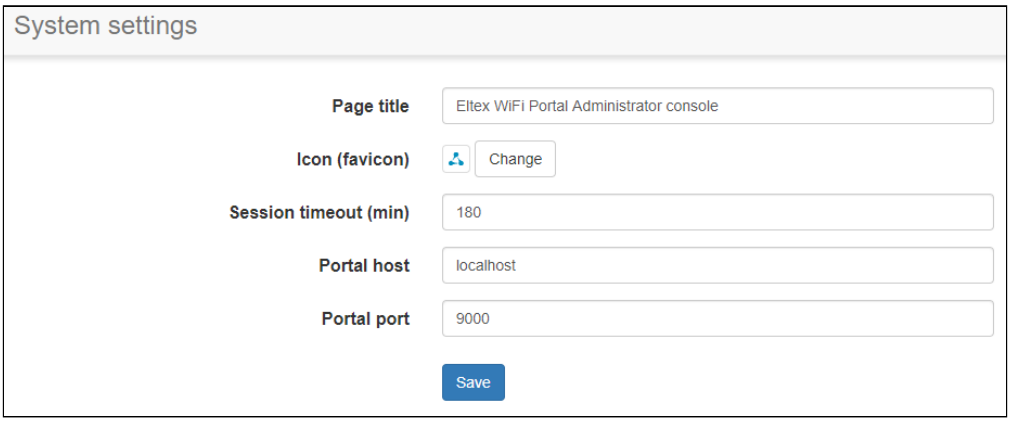
| | |
|---|---|
| **auth-service** — connection to the Auth service | |
| **host** | Authorization service address |
| **port** | a port to which requests will be sent |
| **timeout** | a server's response timeout |
| **retries** | the number of attempts |
| **secret** | a key word for message encryption |
| **protocol** | authorization protocol supported by a server |
| **login** — configuring password sniffing protection | |
| **maxAttemptsLogin** | the number of attempts to authorize under the same login on exceeding of which a Captcha will be enabled |
| **maxAttemptsIP** | the number of attempts to authorize using the same IP address on exceeding of which following attempts will be blocked |
| **blockTime** | IP address blocking time |
| **database** | |
| **host** | Database server address |
| **port** | The port of the database server for getting inbound connections |
| **name** | Database name |
| **user** | Database user's name |
| **password** | Database user's password |
| **readOnly** | Database connection status |
| **pool** | Database connections management<br><br>**connectionTimeout** — timeout of the connection when idle<br>**validationTimeout** — the interval between idle connections validation<br>**min** — the minimum number of connections<br>**max** — the maximum number of connections |
| **cache** | Caching settings<br><br>**maxEntries** — the maximum number of items in the cache<br>**maxResourceBytes** — cache size<br>**expireTime** — cache data storage time |

## System settings in GUI




In this section, integration of the Eltex Portal and the Portal Constructor with platform, advertising and authorization services is configured.

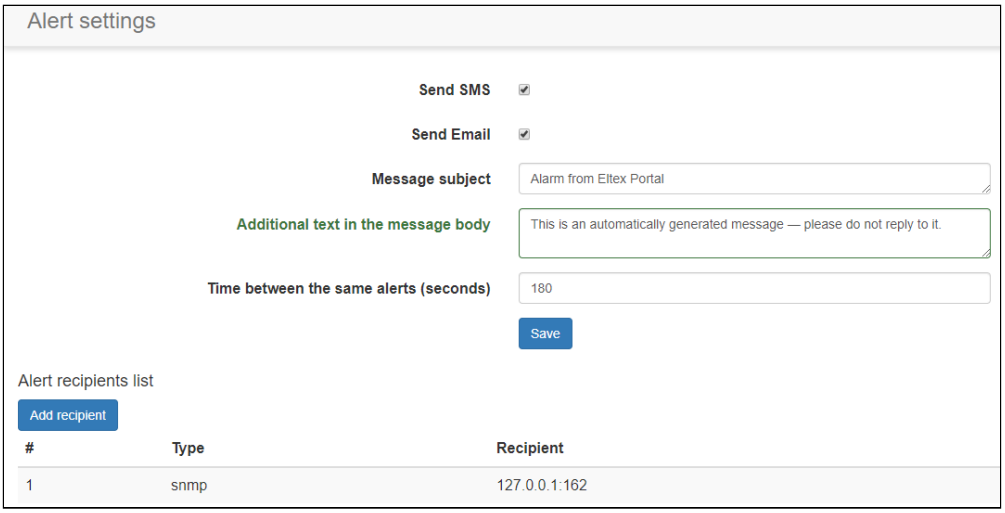
## Portal Constructor




Portal Constructor page setup
Parameters:

- Page title.
- Icon (favicon) — icon displayed in the title.
- Session timeout (min) — idle time on reaching of which a session will be terminated, and reauthorization will be required.
- Portal host — Eltex Portal address used for sending a command on data rereading (applying virtual portal changes without tomcat restarting). This parameter is requires if the Constructor and the Portal are installed on different servers.
- Portal port — a port listened by Eltex Portal service. If the Constructor and the Portal are installed on different servers, they should exchange packets via a specified port (when there is a firewall).

## Alert settings

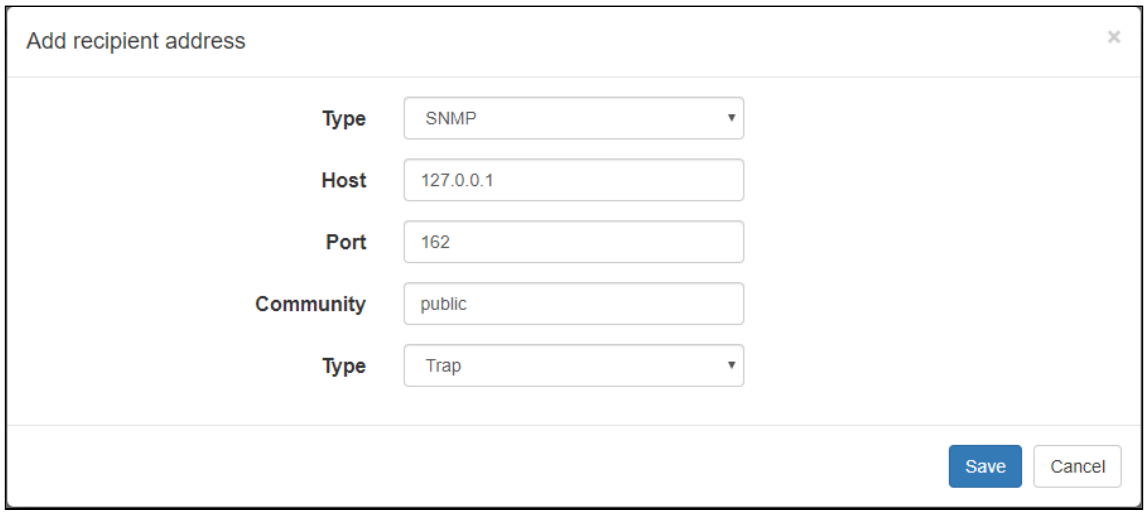



Notification of system administrators on portal operation errors. Notifications are sent by e-mail or SMS. When a new recipient is added, a method of sending messages should be selected. Notifications can be sent via:

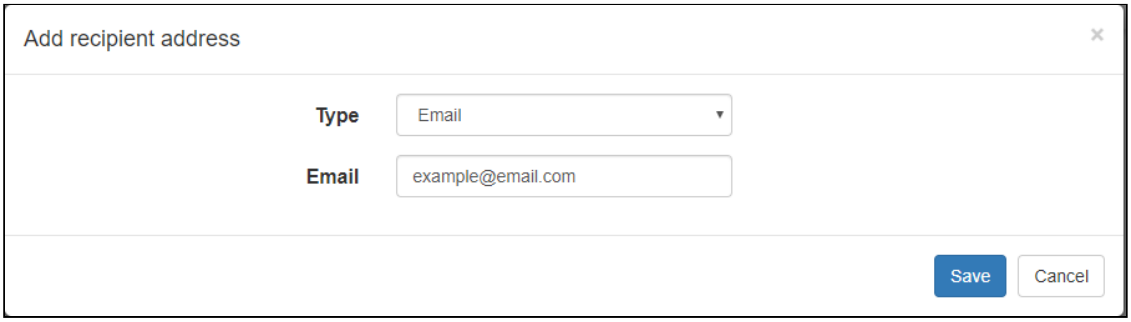
- **SNMP**
- **Email**
- **SMS**

## Notification types

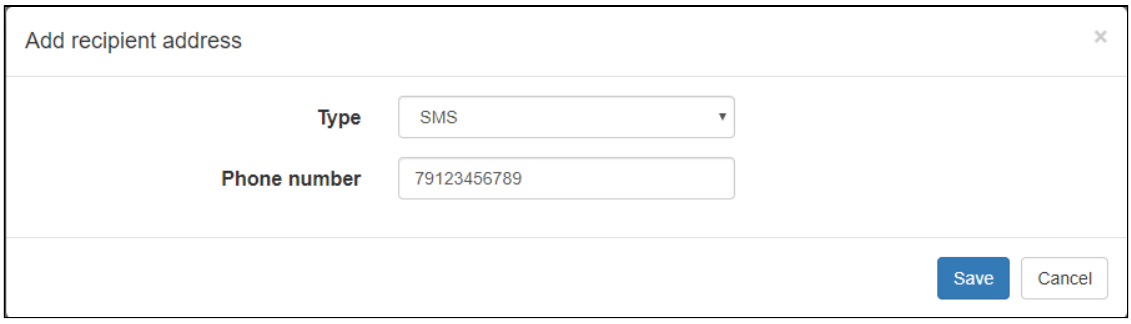
SNMP




E-mail




SMS

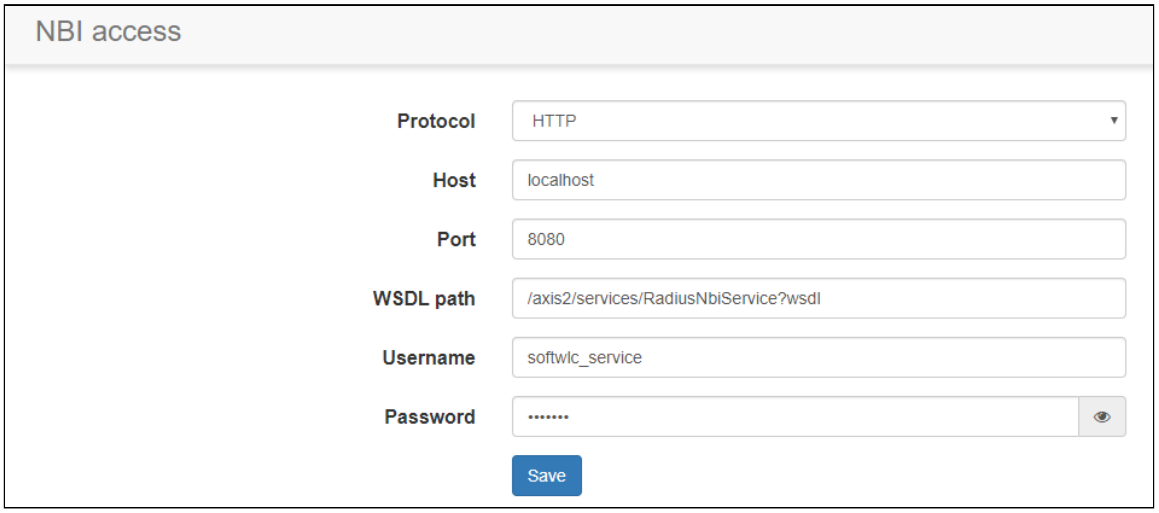



The notification system is intended for notifying SoftWLC users on WEB portal problems. To add a new host, specify the following data:

- **Host** — an address of a server receiving traps;
- **Port** — a number of a port listened by a recipient. 162 port is usually used;
- **Community** — a character string containing a password in the clear;
- **Type (PDU type)** — Trap or Inform;

- **Response timeout (seconds)** — recipient response timeout (for Inform only);
- **Number of attempts** — the number of attempts to send messages of Inform type with an interval equal to the timeout.

NBI access

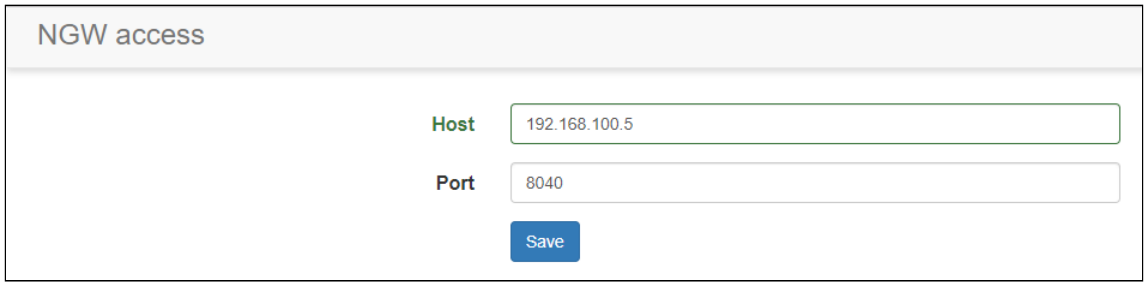



The interface to provide interaction between SoftWLC components
For the Portal to work correctly, configure its connection to the EMS server via Northbound interface. It allows the Portal Constructor to get all required data from EMS, for example a list of tariffs and their parameters.
Parameters:

- Protocol — a protocol used to transmit data to NBI (HTTP or HTTPS). A protocol is selected depending on the NBI configuration on the NBI server.
- Host — NBI server's address;
- Port — a port listened by NBI;
- WSDL path — an address on the server where the WDSL file is located. As a rule, it is "/axis2/services/RadiusNbiService?wsdl";
- Username — user login;
- Password — user password;

To access NBI, a service account **softwlc_service/service** should be used.

NGW access



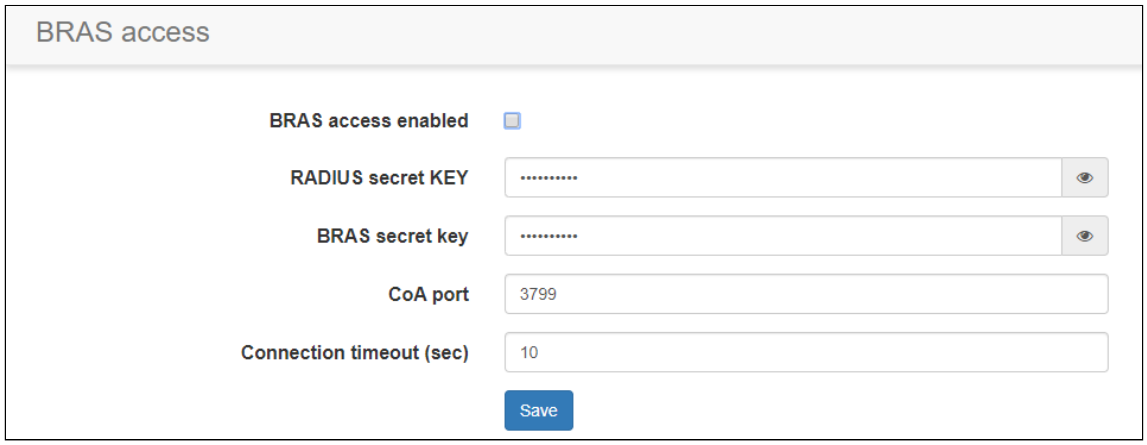

an interface for working with SMS gateways.

Parameters for interaction between the Portal Constructor and the Notification Gateway service are configured in this section. It is necessary for the Constructor to be able to read information on support for different authorization types from NGW. As a result, if NGW is not configured for the call back authorization, the Portal Constructor will not offer this option to a user.

Parameters:

- Host — NGW server's address. If the Portal Constructor and NGW are installed on the same server, the field should be filled in with "localhost".
- Port — a port listened by NGW.

BRAS access



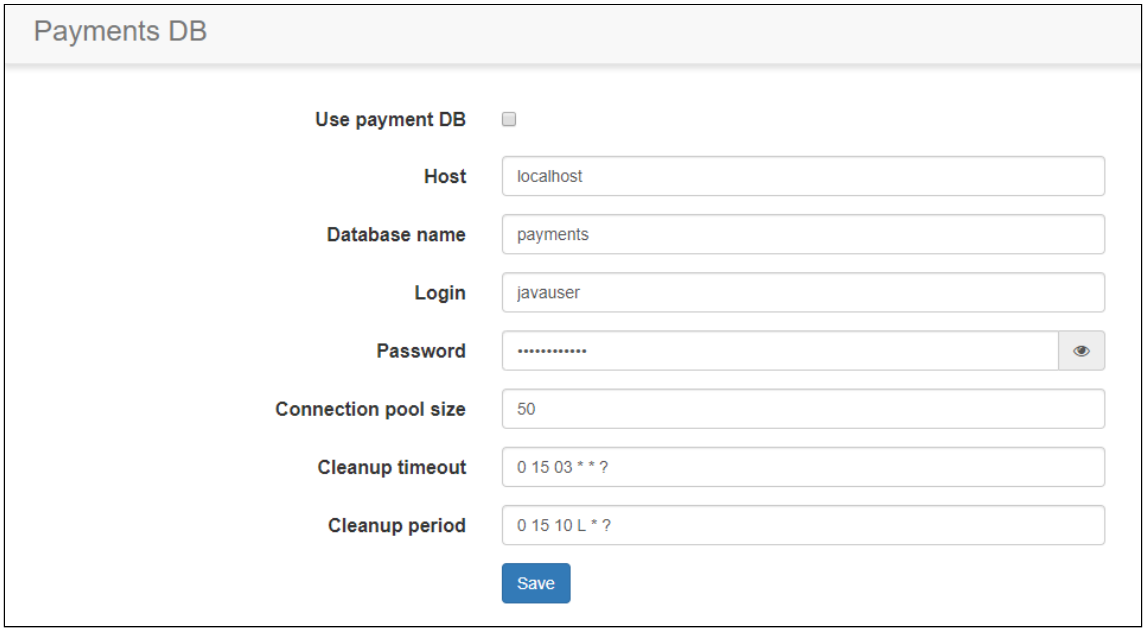

BRAS access settings.

When a checkbox "BRAS access enabled" is checked, BRAS support is activated on the Portal.  After BRAS activation, PCRF tariffs will be available in portal settings.

Parameters:

- RADIUS secret KEY — a password used for exchange with RADIUS;
- BRAS secret KEY — a password used for CoA message exchange;
- CoA port — a port used for message exchange;
- Connection timeout (sec) — response timeout;
- Connection pool size — device number limit on BRAS.

Payments DB



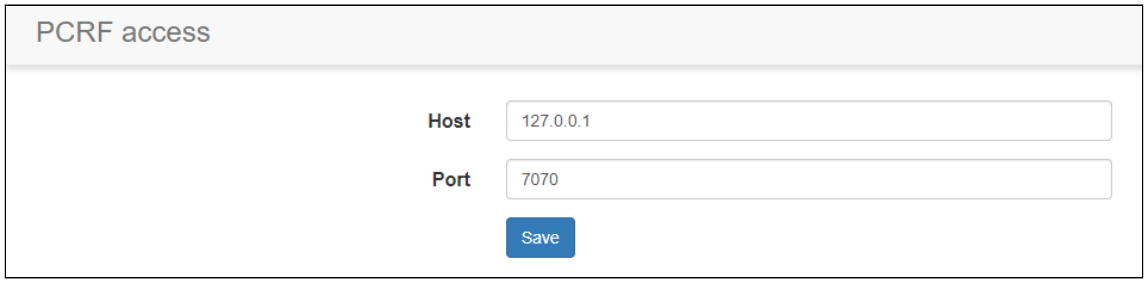

access to the database containing information on tariff payment status.

When the checkbox "Use payment DB" is checked, the Portal initiates interaction with the database to store information on users' payments. If the checkbox is not checked, paid tariffs cannot be used.

Parameters:

- Host — the database server's address;
- Database name;
- Login — a login for the database access;
- Password — a password for the database access;
- Connection pool size — the maximum number of devices that can be connected to the database at the same time;
- Cleanup timeout — a timeout for irrelevant connections checking and deleting;
- Cleanup period — a timeout for deleting old entries from the database.

PCRF access

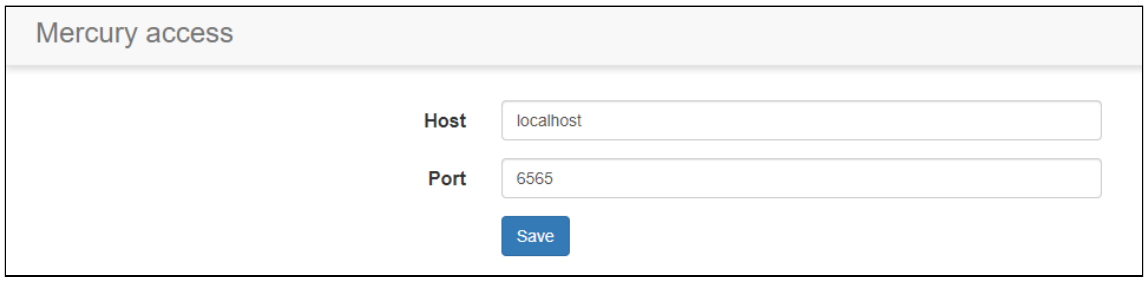



access to the session billing system for subscribers connected via BRAS.

Parameters:

- Host — PCRF server's address;
- Port — a port listed by PCRF.

Mercury access

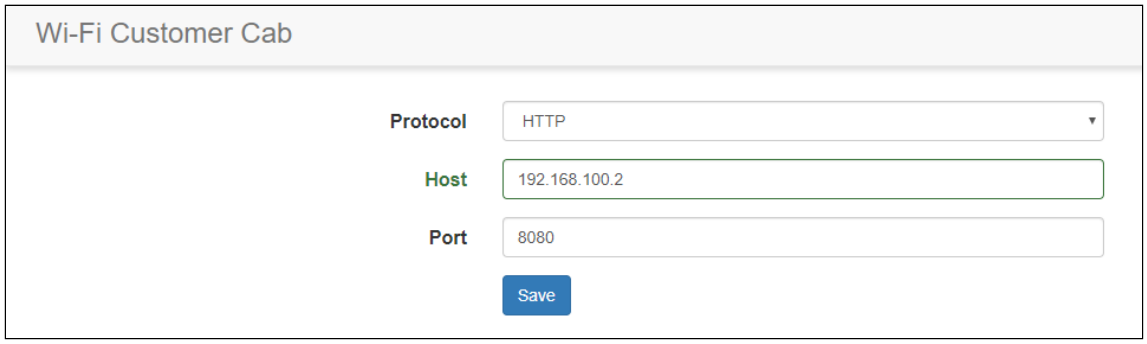



access to the user account management service eltex-mercury

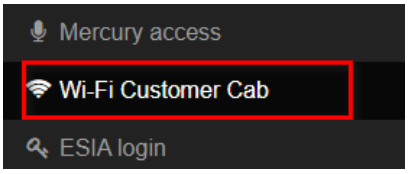
Parameters:

- Host — Mercury server's address;
- Port — a port listed by Mercury.

Wi-Fi Customer Cab (Admin Panel)



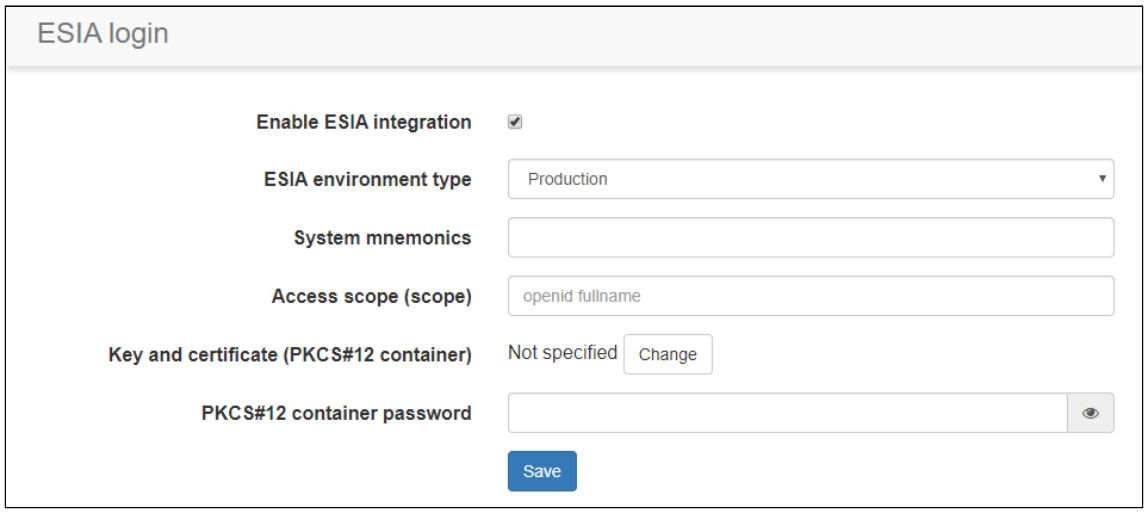

The link to Wi-Fi B2B Admin Panel. The link is displayed on the control panel of the Portal Constructor.




Parameters:

- Protocol — a protocol used for interaction with the Admin Panel (HTTP/HTTPS);
- Host — the Admin Panel server's address for users to be able to connect from an external network;
- Port — a port listened by the Admin Panel server.

ESIA login



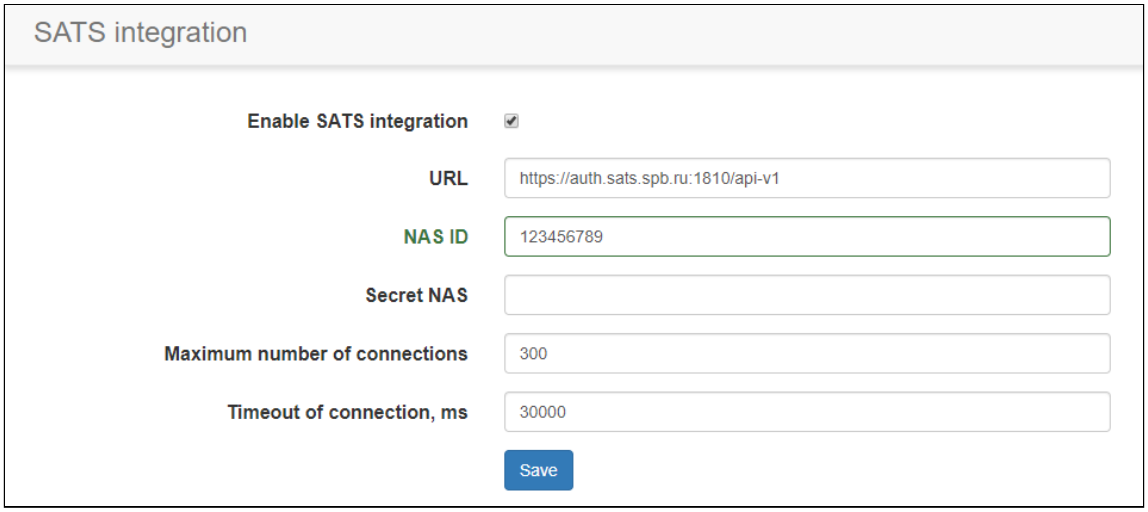

ESIA integration configuration.

Parameters:

- ESIA environment type — Production or Test;
- System mnemonics — system identifier in ESIA;

- Access scope (scope) — operations that can be performed by a system (Eltex Portal in the present case) on behalf of a user;
- Key and certificate (PKCS#12 container) — system certificate registered in ESIA during application;
- PKCS#12 container password — a private key to a container with the certificate.

SATS integration




Configure SATS integration to perform MAC authorization using a common database of other providers.

Parameters:

**Enable SATS integration** — SATS integration opportunity for a portal; It is necessary to check an additional checkbox for each virtual portal;

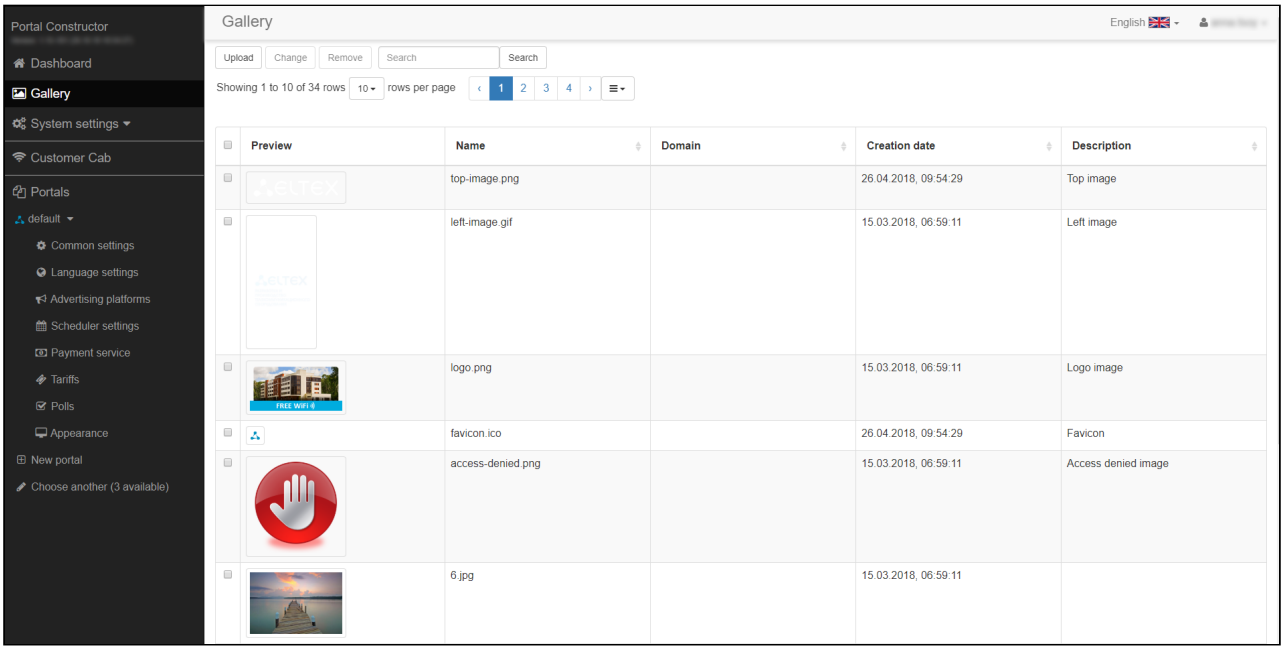
**Maximum number of connections** — the maximum number of connections Eltex portal can hold to interact with SATS;

**Timeout of connection, ms** — the authorization service response timeout;

**NAS ID** — an individual identifier used in service authorization requests;

**Secret NAS** — a sequence used for sending requests to the authorization service.

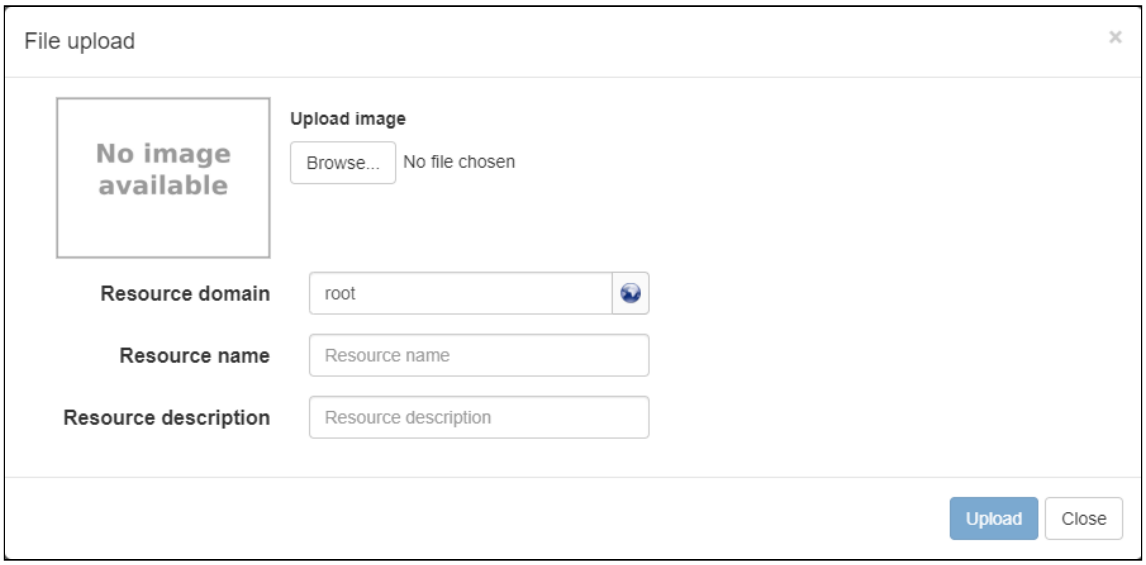
## Gallery




All images imported to the Portal Constructor and used for virtual portals' pages configuration are stored in the Gallery.

Search can be performed directly on the table columns: Name, Domain, Description.

## Adding/updating images



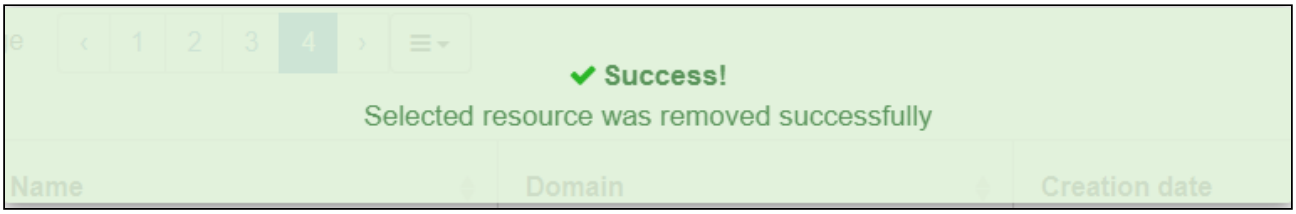

Images can be added to the Gallery during virtual portals configuration (when images are selected) and directly in the Gallery. Process of adding an image to the Gallery:

1. Click "Upload".
2. Select a required image in the opened window.
3. Specify a Resource domain and add a Resource description. Resource domain is a domain of an image visibility for a Portal Constructor user. Portal Constructor users can see images with a domain that matches a user account domain or is a subdomain of it. Default images that are available in the Portal Constructor since the installation and do not have a domain, are visible for all Portal Constructor users.

After that, a new image will be added to the Gallery.

Parameters of an already added image can be changed. To do that, select an element and click "Change". If several elements are selected, the button "Change" will be unavailable.
When Name, Domain, Preview or Description of an element is changed, a link between the element and portals continues to exist. Thus, it is possible to add the same element to several different portals and then to make changes that will be applied to all cases.

### Deleting images



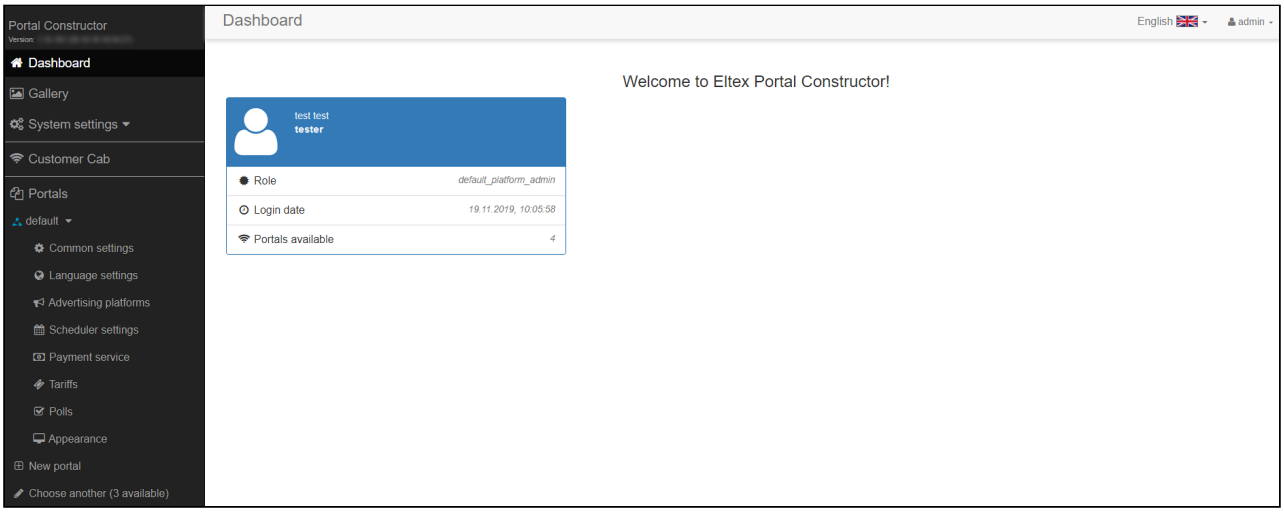


To delete images from the Gallery, select them and click "Remove".

When being deleted, an image is checked for being used anywhere else. If it is not, the system will display a message stating that the image has been deleted successfully.

If some of the images being deleted are used somewhere else, a list of corresponding virtual portals will be displayed.

## Dashboard




Portal Constructor welcome page. The following parameters are displayed on the Dashboard:

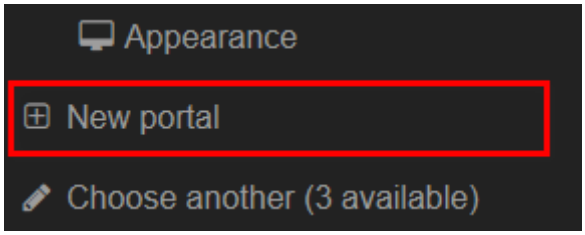
- First name, Last name and Login of a user;
- User role (is not displayed for 'admin');
- Time of the last entry;
- The number of available portals (located in a user's domain);
- The number of portals without tariffs (user authorization is not available for these portals).

## Customer Cab

The tab "Customer Cab" located on the side bar of the Portal Constructor is intended for fast and convenient switching between the Portal Constructor and the Admin Panel. As authorization in the Portal Constructor and the Admin Panel is performed via the same system: Auth Service, the Admin Panel is opened in a new browser tab after clicking the "Customer Cab". Authorization is not required as it is performed automatically.

## Portals

### Creating a new portal

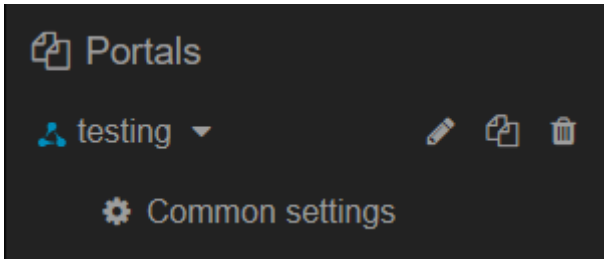




To create a new portal, click "**New portal**" on the side bar of the Portal Constructor. It is necessary to specify a Name and a Domain when creating a new portal. Portal Name will be required during an access point's Virtual Portal Name SSID configuration to link the SSID to a customized portal. Portal Domain will define Portal Constructor users for whom a portal will be visible (Portal domain should match a domain of a Portal Constructor user's account or be its subdomain). A WEB portal can contain an unlimited number of pages (portals) with unique customization.

The Portal Constructor has the "Default" portal after installation. This portal is available only for the Portal Constructor Administrator. When a new portal is created in the Portal Constructor, it has the same configuration as the "Default" portal has. Therefore, the Administrator can configure the "Default" portal for other portals to be initially pre-configured and to require the minimum efforts for their customization.

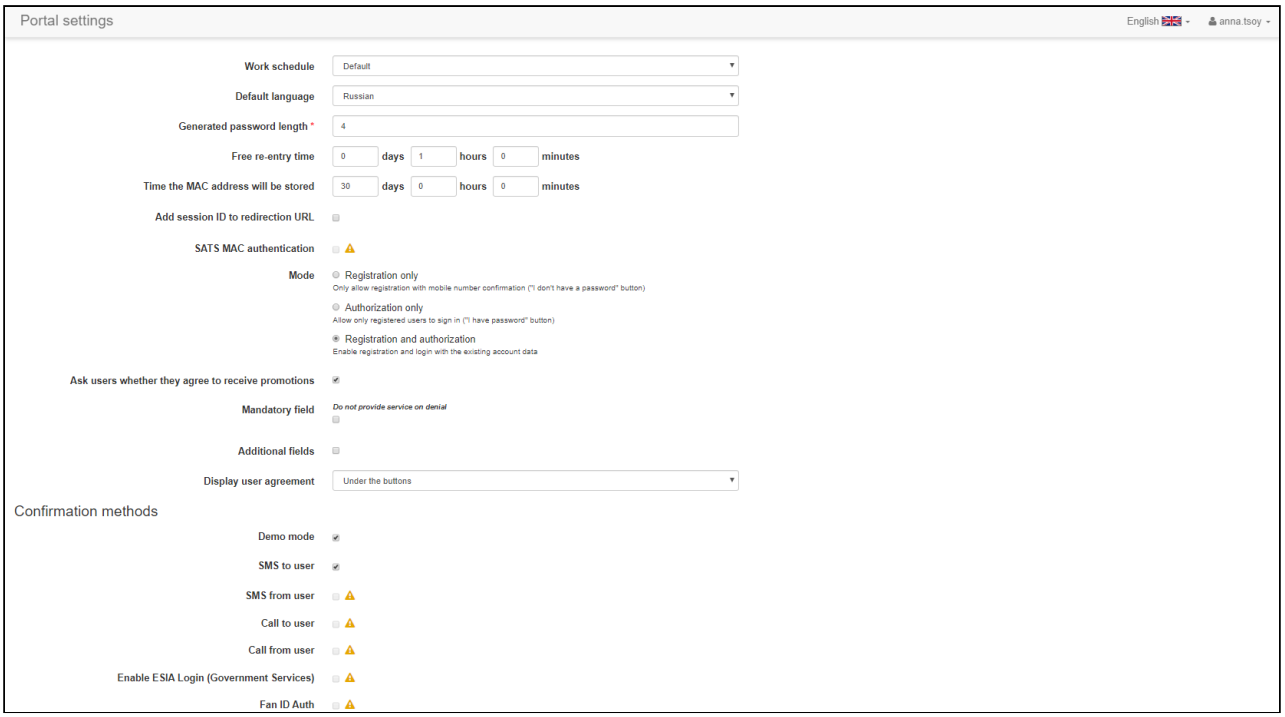
## Copying a portal

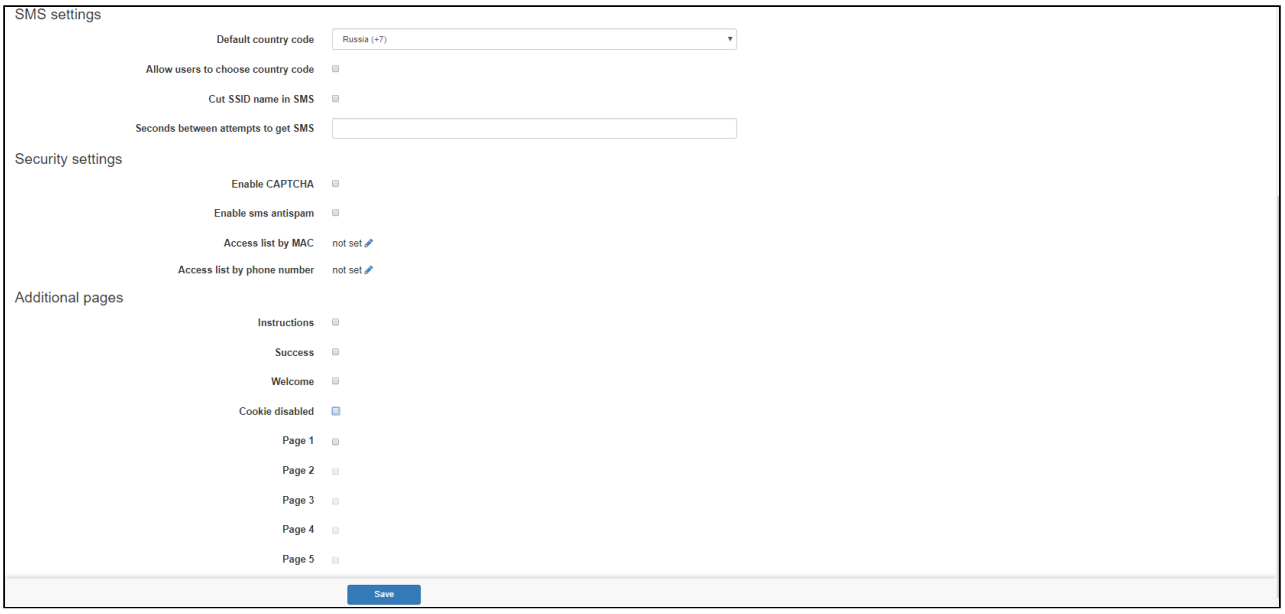



To copy a portal, click  . The following data will be copied:

- Portal settings
- Portal appearance
- Portal domain

## Common settings




In the section "Common settings" main parameters of a portal are configured.

**Language settings** — a language used by default when a portal is opened on a client's device, if a language used on it is not supported by a portal. Language can be defined by headers transmitted by a

user's device (the field Accept-Language). Many devices transmit several languages in this field. If one of transmitted languages is supported by a portal, it will be used instead of the main language.

**Generated password length** — a number of symbols in a password generated automatically during user registration.

**Free re-entry time** — sets time during which a user will not return to a portal (the Welcome page) when reconnected (relevant for the scheme of connection via BRAS).

**Add session ID to redirection URL —** adds a unique user session identifier to a URL when redirection from a portal is performed. Session ID substitution is put to URL in the following cases: Redirection from the final page and click on a banner on the "Sussess" page.

**Time the MAC address will be stored** — defines a user's MAC address storage period. When a user is reconnected, the system identifies a user automatically, without re-registration on the portal.

**Enable ESIA Login (Government Services)** — enables a form for user authorization via ESIA. The option is available only if integration between Notification GW and ESIA is implemented.

**SATS MAC authentication** — enables checking SATS for a user's MAC address. The checkbox is available only if integration with SATS is enabled on a global level.

**Mode** — selecting a user authorization mode. Available modes:

**Registration only** — if this mode is selected, a Wi-Fi user will be able to authorize in the system only after phone number confirmation (for example, by specifying it on a portal and receiving an SMS with a password). A user will not be able to specify credentials obtained in advance. The mode is typical for classic hotspots with call back or SMS authorization.

**Authorization only** — a Wi-Fi user will be able to authorize on a portal only if he enters a login and a password issued in advance into a special form. It will be impossible to perform authorization by confirming a phone number via a call or an SMS. Logins and passwords are usually generated by an organization Administrator.

**Registration and authorization** — the composition of the modes described above. A user can: enter credentials received in advance or register a phone number via an SMS or a call (see below for details).

**Ask users whether they agree to receive promotions** — display a checkbox to define if users agree to receive promotions.

**Mandatory field** — allows to make an agreement to receive promotions obligatory. If a checkbox is checked, a user should agree to receive promotions to authorize on a portal (otherwise the services will not be provided).

**Additional fields** — the option allows getting additional information on users: first name, last name, e-mail address. If the checkbox "Mandatory field" is checked, the fields are obligatory to be filled in (the option is not supported if the payment service is enabled).

**Confirmation methods** — select a way for a user to confirm his phone number. Several methods can be enabled. Then a user will be able to choose the most appropriate method.

**Demo mode** — the mode that does nor require integration between Notification GW and other systems. The mode allows learning about a portal operation on initial steps of the system installation. When a user selects this mode and enters his phone number, a portal page is opened with the field "Login" filled in with the phone number, and the field "Password" filled in with an automatically generated password. A user should click the button "Log in" to perform authorization. No SMS are needed. *However, this mode*

*does not provide subscriber identification, as a subscriber may enter a phone number that does not belong to him and stay anonymous. It is recommended to use this mode for demonstration purposes, not for real operation, as it may contradict the laws of a country in which the service is provided.*

**SMS to user** — confirm a phone number by sending an SMS with a password to a user. A user should enter his phone number on a portal for the system to generate a password and send it via SMS. A user enters this password on a portal's page (with the field "Login" filled in with his phone number) and thereby performs authorization and confirms the phone number. The mode requires integration between Notification GW and an SMS gateway of a provider used for SMS sending.

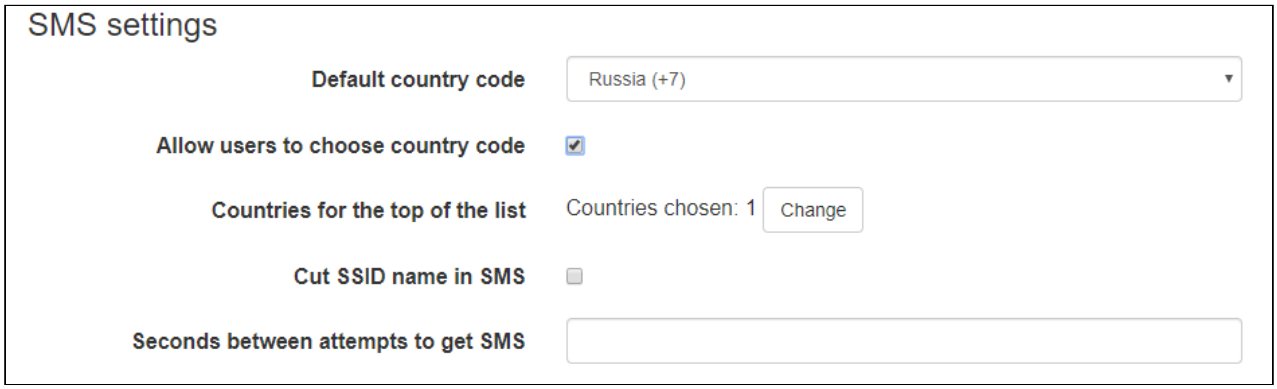
**Call to user** — confirm (register) a user account via a call back.

- Response timeout (s) — SMG gateway response timeout. Can be from 10 to 600 seconds.

**SMS from user**
**Call from user** — confirm (register) a user account via an outgoing call.

**Additional pages** — additional pages of a virtual portal used to organise switching between complex scenarios and user notifications.
**Instructions** — enable instructions on portal pages.
**Success** — enable a success page seen when the Internet connection works.
**Page 1-5** — enable additional pages of a virtual portal.

SMS settings




**Default country code** — phone numbers of foreign users have prefixes different than "+7". A user have an opportunity to select a prefix of his country on a portal. The option is used to select a prefix displayed by default after a portal launch.

**Allow users to choose country code** — enables/disables country code selection on a portal. If the option is disabled, a user will be able to specify a phone number only with the default prefix. The option is usually enabled when people from other countries are expected to authorize on a portal.

**Countries for the top of the list** — creation of a list with phone codes of countries that will be displayed in the top of the list containing all country codes. The option is available in Common settings only if the option "Allow users to choose country code" is enabled. The option is commonly used to put phone codes of countries frequently selected during portal authorization in the top of the list. As a result, most users do not have to scroll the list to the end — required prefixes can be found at the top.

**Cut SSID name in SMS** — the option allows reducing the length of SMS sent to a user by SSID name shortening (if it is too long) in order to fit information into one message. That helps to save on SMS sending.

## Security settings



**Enable CAPTCHA** — enable captcha on a portal to provide bot protection.

**Captcha length** — the number of symbols in a captcha image. The higher is a number of symbols, the higher protection from bots, and the more complicated a procedure of captcha entering is for a user. The option is displayed in the settings only if the option "Enable CAPTCHA" is activated.

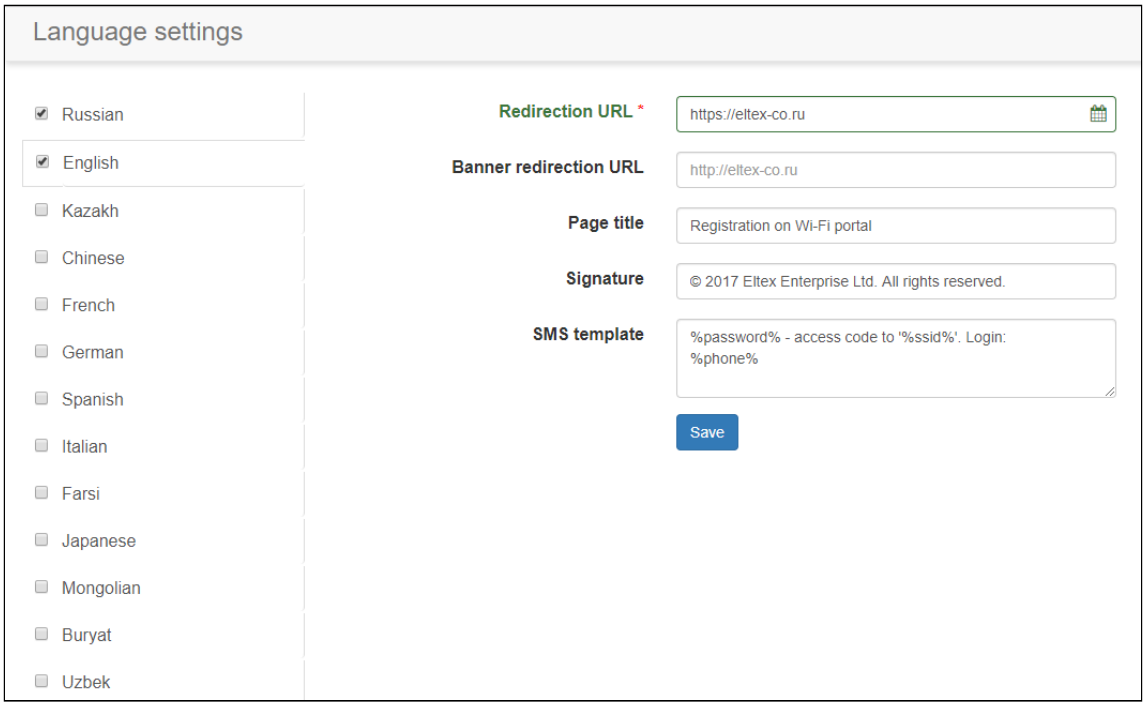
**Enable sms antispam** — the option limiting a frequency of sending SMS to a user. If the limit is exceeded, a user will be banned (by MAC address) and will not be able to authorize. If authorization is successful, the counter is reset. After enabling the option, there will be an opportunity to set a number of attempts to receive an SMS message on exceeding of which a user is banned, time between attempts (in seconds) and a period during which a user is banned.

**Access list by MAC** — list of MAC addresses that allows limiting access to a portal by a client's MAC address. There are two types of lists:

- White lists — all addresses contained in the list, have access to a portal while others do not. If a client's MAC address is not contained in a white list, he will get a page of the portal explaining that there is no such MAC address in the list.
- Black lists — all addresses have access to the portal while addresses included into a list do not. If a client's MAC address is contained in a black list, he will get a page of the portal explaining that the MAC address is contained in the list.

**Access list by phone number** — the list containing phone numbers and used to limit access to a portal by a client's number.

## Language settings




The portal can simultaneously support several languages: Russian, English, Kazakh, Chinese, German, Italian, Farsi, French and Spanish.

A user can select languages in the left side panel by checking corresponding checkboxes. The two languages are available by default. English and Russian. Other languages are initially disabled. If there was an upgrade from previous SoftWLC versions, language settings of portals created before remain the same.

The following settings are available for each language:

**Redirection URL** — URL of a page to which a user will be redirected after portal authorization (for example, when he has entered a phone number, received an SMS and specified a password on the portal,

he will be automatically redirected to this URL). It is usually a client's (or a provider's) website or an advertising page.

> ⚠ Cyrillic domains should be previously converted, for example, using https://2ip.ru/punycode/. Paste a new link to the **Redirection URL**.

**Page title** — is formed by a portal administrator individually (an optional parameter).

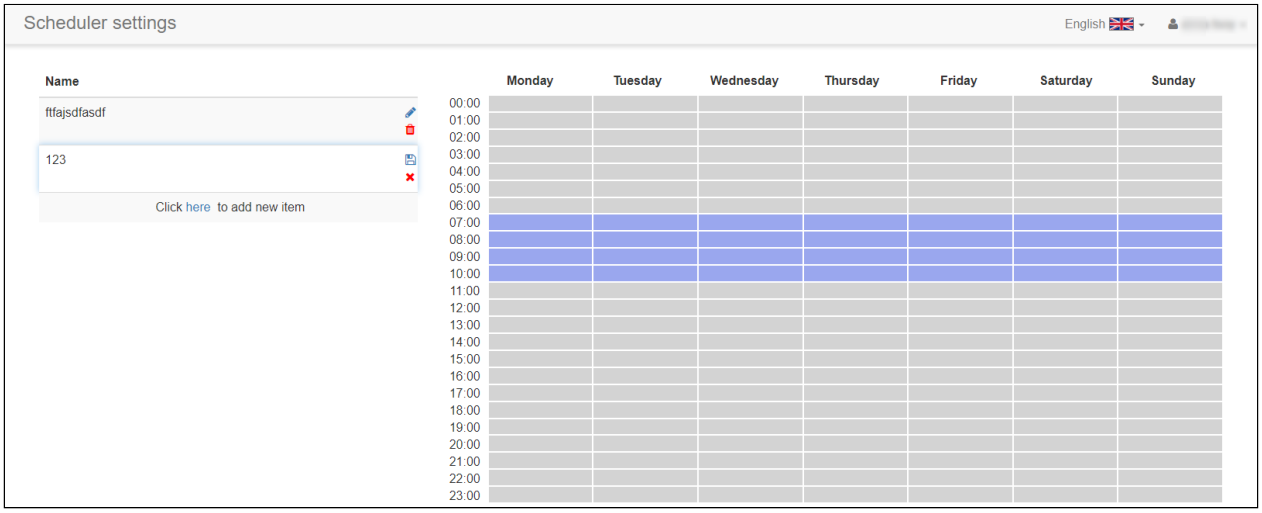
**Signature** — is formed by a portal administrator individually (an optional parameter).

**Message on successful connection** — text of a message.

**SMS template** — a template for a message in which a password will be sent to a user.

## Scheduler settings

### Expanded schedule




The section allows creating schedules. They are used for configuring banner displaying and URLs to which users are redirected after portal authorization.

> ⚠ To create and edit schedules, a Portal Constructor user should have rights to edit system settings. Created schedules are available for all users.

To view and edit a schedule, click the icon on the right from a schedule's name. After that, it will be possible to select working hours for this schedule. Working hours are displayed as coloured cells, off hours — as light grey cells.

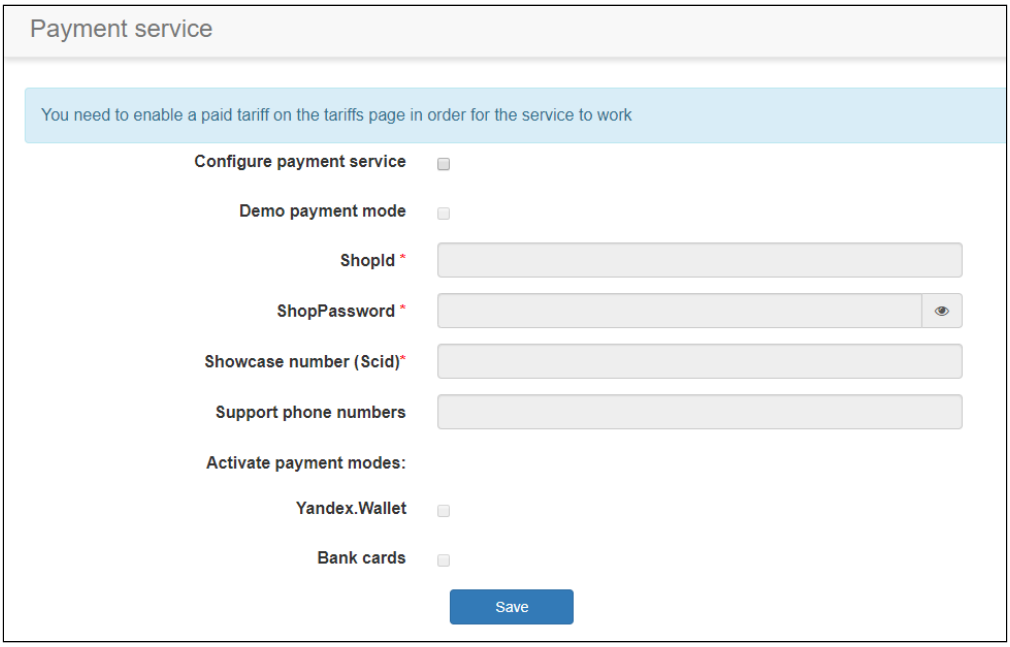
To save changes, click the icon . To cancel changes, click .

To delete changes, click . When a schedule is deleted, all resource (banners and redirect URLs) links to this schedule are deleted on all portals where it is used.

To add a new schedule, click the link "here".

> ⚠ The buttons for saving changes and deleting schedules will not be displayed for users without editing rights.

## Payment service




A user can be authorized on a portal only after making a payment via the service Yandex.Checkout.

To enable payment services, check the checkbox "Configure payment service".

**Demo payment mode** — enable/disable demo mode for Yandex.Checkout;

**ShopId** — a unique portal identifier in the payment service system. ShopID can be obtained after Yandex.Checkout registration**(obligatory field)**;

**ShopPassword** — portal password in the payment service system. ShopPassword is specified independently in a Yandex.Checkout account **(obligatory field)**;

**Showcase number (Scid)** — a showcase number in the payment service system. Scid can be obtained after Yandex.Checkout registration **(obligatory field)**;

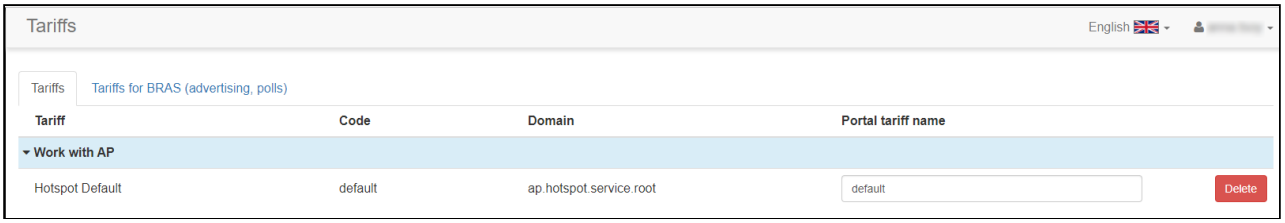
**Support phone numbers for payment failure cases** — a number of technical support will be displayed if the field is filled in, but a payment has been declined for some reasons, and a user has been redirected to the portal from a payment website;

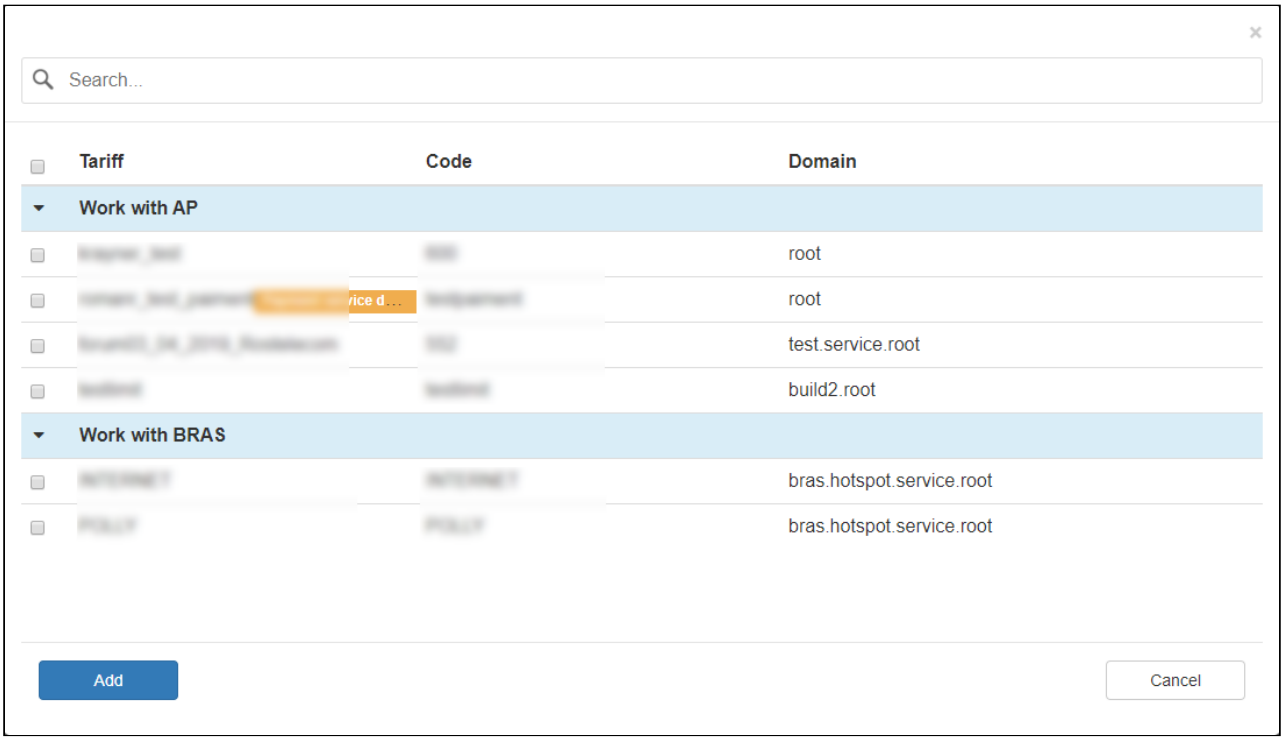
**Activate payment modes** — enable/disable payment methods. Available payment methods are listed in the section "Payments" on checkout.yandex.com. The following payment methods can be enabled:

- Yandex.Wallet (available in the demo mode);
- Bank cards (available in the demo mode);
- Alfa-Click;
- Sberbank Online or Sberbank SMS;
- Payment terminals;
- WebMoney;
- Qiwi wallet;
- Direct carrier billing.

> ⚠ If no paid tariffs are configured on a portal, the following message will be displayed on the page "Payment service":
> 'You need to enable a paid tariff on the "Tariffs" page in order for the service to work'

## Tariffs





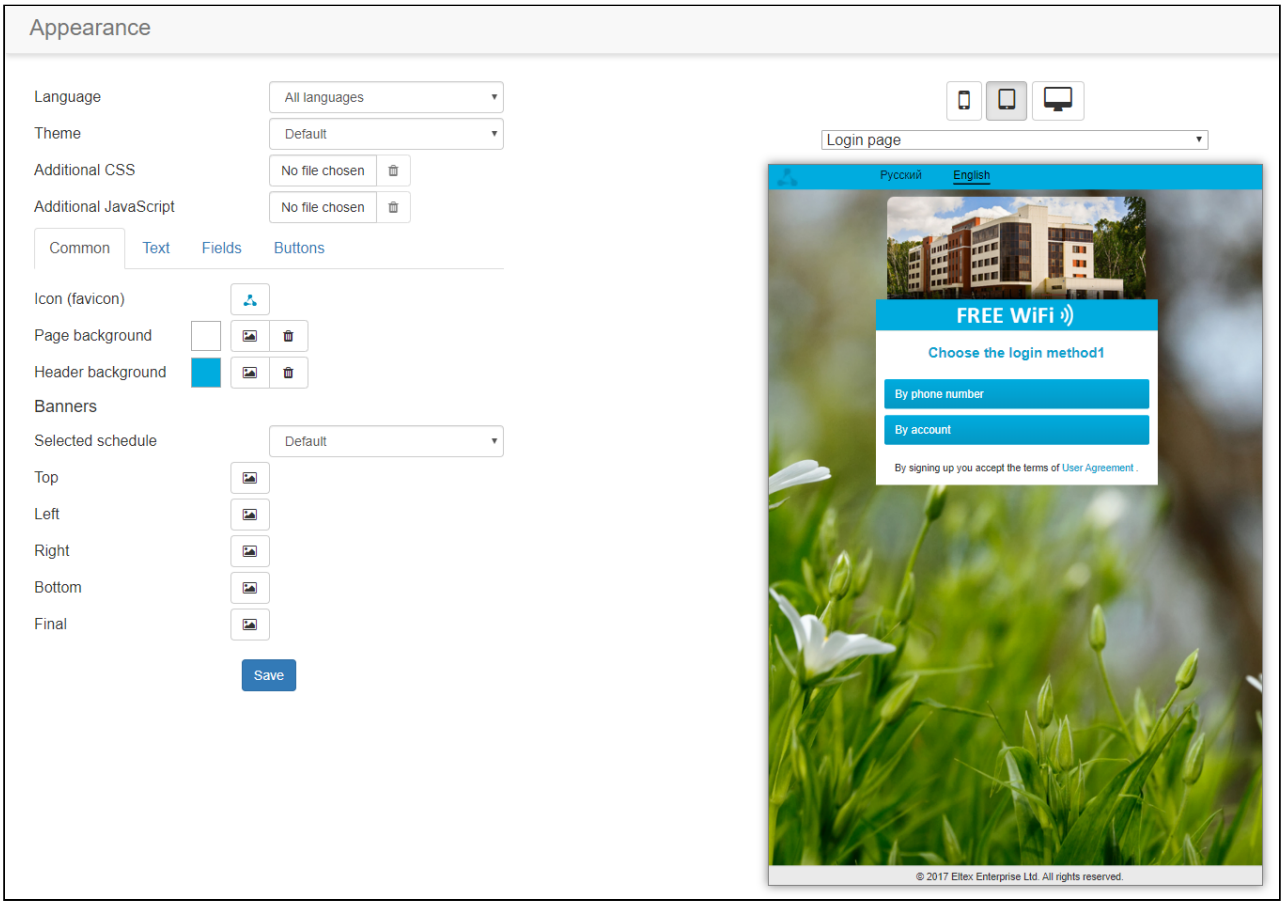

Tariffs that contain access limits and are offered to users on connection to a SSID in Hotspot mode which a considered WEB portal relates are selected on this tab.

In the field *"Portal tariff name"*, a tariff name seen by a user during portal registration can be specified. Tariffs for "Access points" are configured via the Admin Panel or via the system Eltex.EMS. PCRF tariffs can be configured only via the Admin Panel.  Several tariffs can be configured within one portal.

A portal should have at least one tariff. Otherwise, a portal will now be able to operate, and an error will be displayed on users' devices.

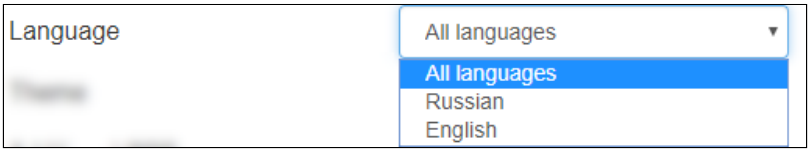
To add a new tariff, click the button "Add". Select tariffs by checking corresponding checkboxes. Click the button "Add" in the current window to confirm the choice.

## Appearance



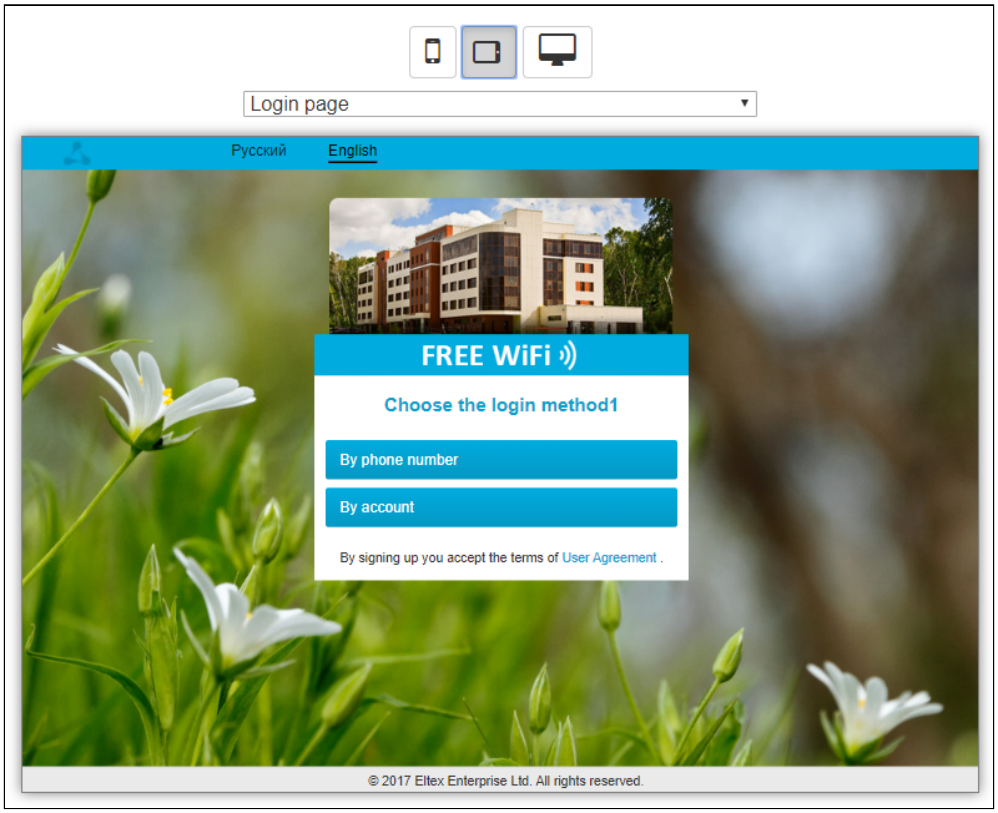

A toolkit for changing appearance and content of portal pages.

## Language




The virtual portal has a multi-language interface. A Wi-Fi user can select any language from the offered ones. In order to configure portal pages' appearance separately for each language, the language selection menu is used. When a certain language is selected, all changes will be applied only to this language. Thus, when a content of text fields is edited, changes will be saved only for the language which is selected. When the mode "All languages" is selected, changes will be applied to all available languages.

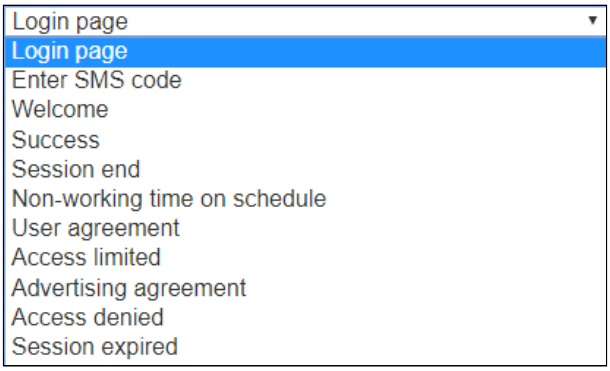
## Preview



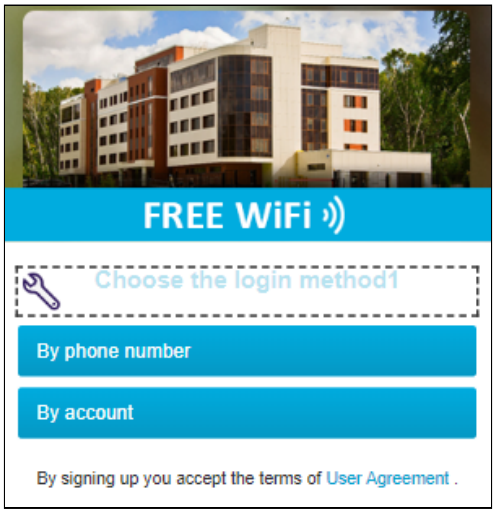

The preview is used to configure a portal and to see how a virtual portal is displayed on users' devices. The preview is located in the right part of the configuration window. Above the preview, the following icons are displayed:  . They are used to switch a client device type and to show how a portal will look on a smartphone, tablet or laptop screen. To see how a portal will be displayed for screen landscape orientation, left-click the icon twice:  .

Below the icons, the menu for portal page selection is located 

. During portal authorization, different pages of a portal responsible for a certain authorization step are displayed on a subscriber's device (Login page, Enter SMS code, Session end, Non-working time on schedule, User agreement, Access limited, Access denied, Session expired):

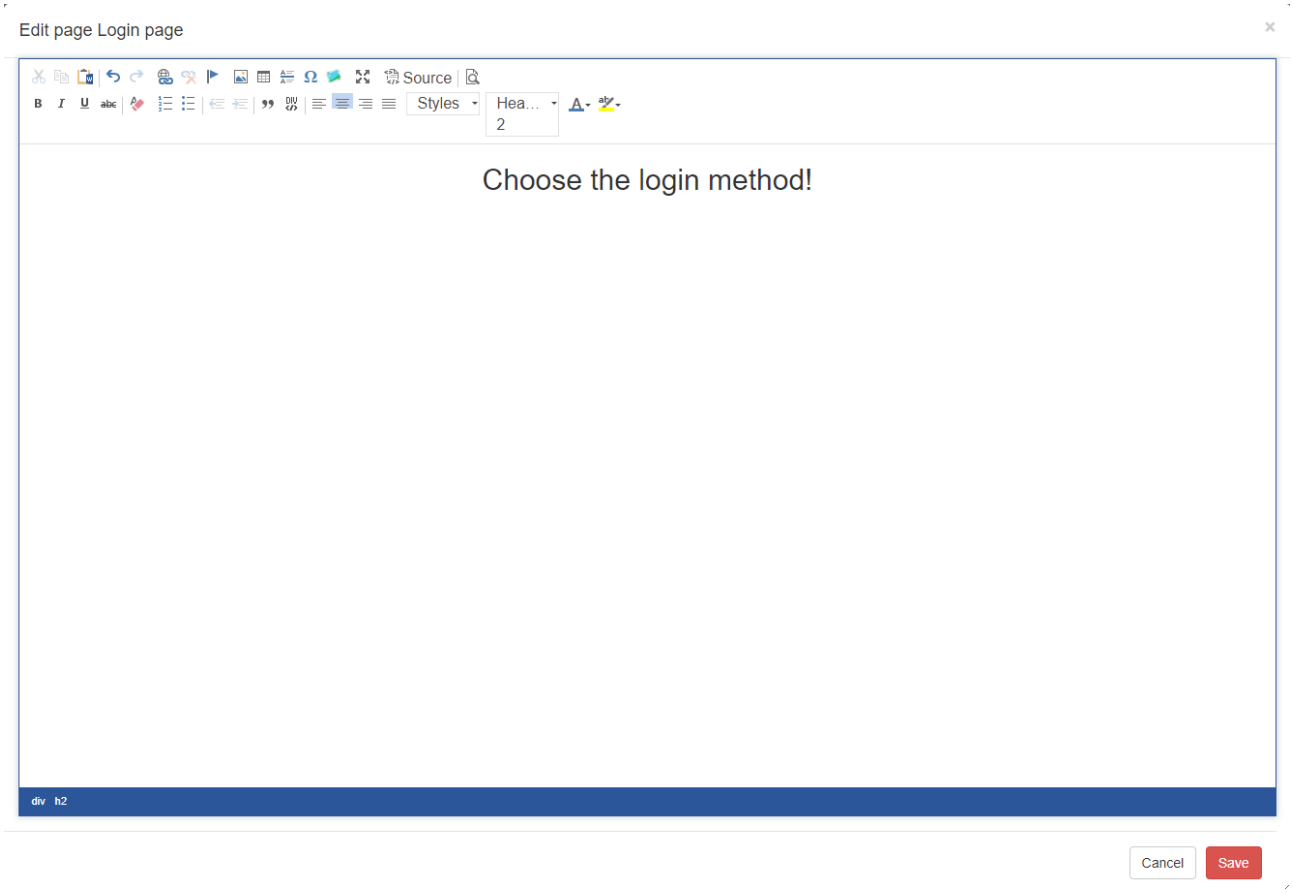



Configuring elements

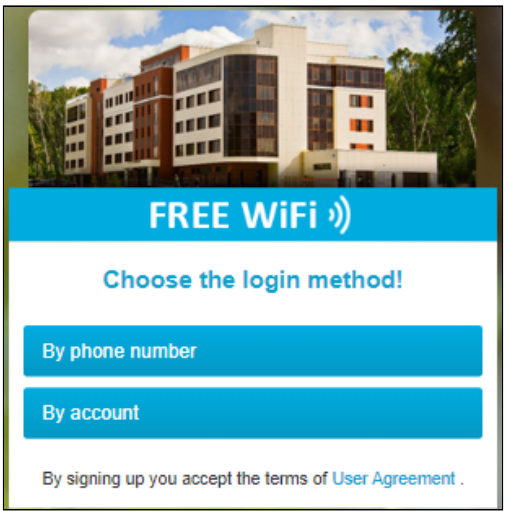



Example of editing a message on a welcome page

Click the image of a wrench to edit a welcome text:




As a result, a portal will look like this:



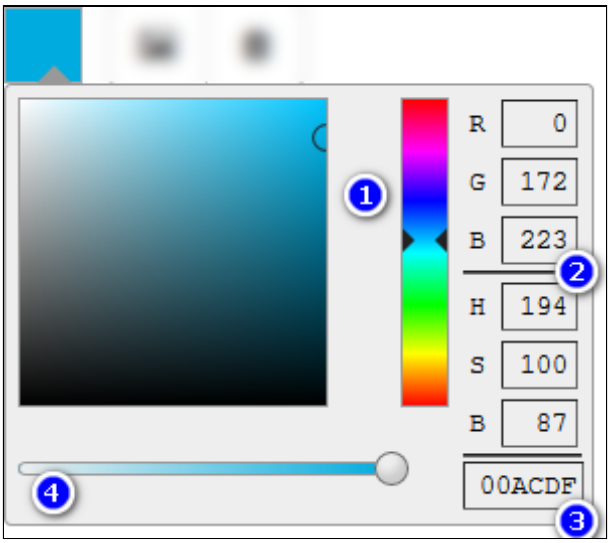

When hovering a mouse over portal elements in

the preview, a special icon

be noticed. That means the element can be changed by a user. This option is available for portal text fields and images used for banners. Note that content of some text fields is standard for all portals, for example, explanatory texts displayed during registration/authorization. Such texts are non-editable. Moreover, the text of the "User agreement" should be changed centrally for the whole system, so it can be edited only by a superuser and only in the portal "default" from which other portals will obtain it.

Configuration tools

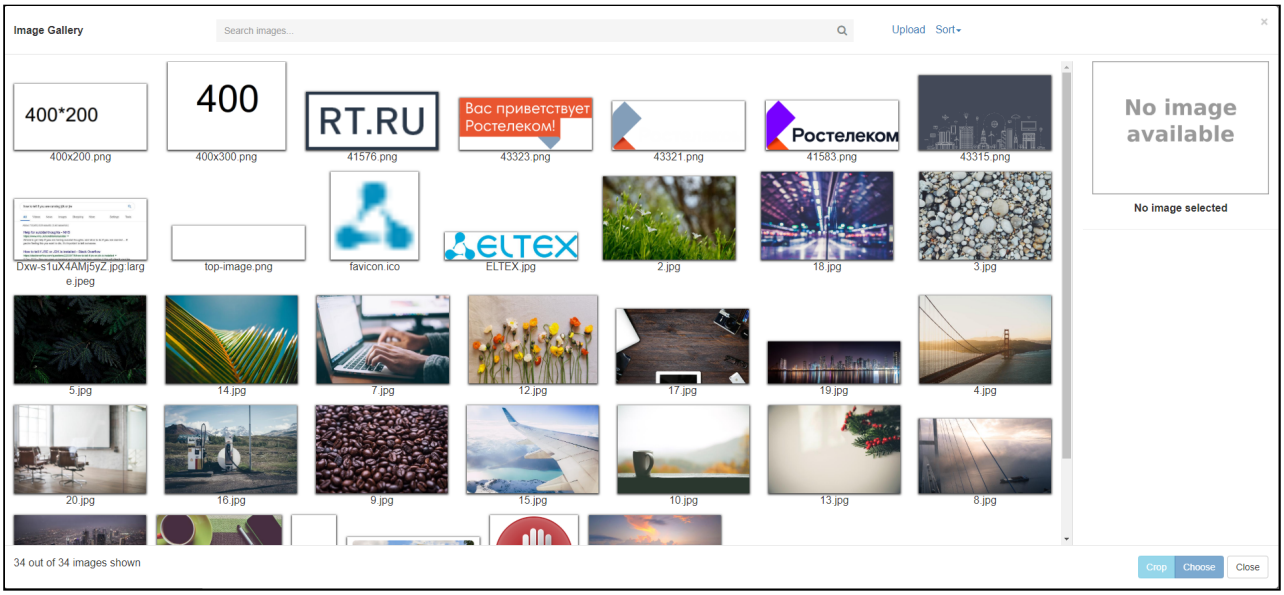
Colour settings




To change a colour of elements, click the icon looking like a filled square (shows the current colour): . The window for colour selecting will be opened. The elements of the window:

1. Palette — shows a selected colour and gives an opportunity to select a colour by clicking on a required point of the palette square.
2. Colour RGB/HSB code — combination of integer values.
3. Index — colour representation in a form of an index. A colour index can be specified manually.
4. Saturation — move the slider to change colour transparency from 0% (transparent) to 100% (opaque).

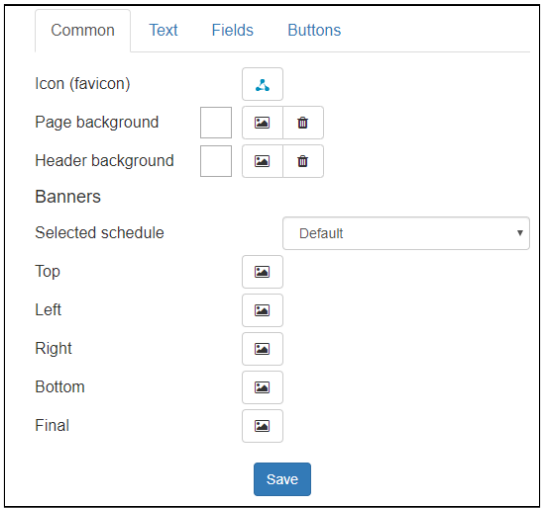
Selecting an image

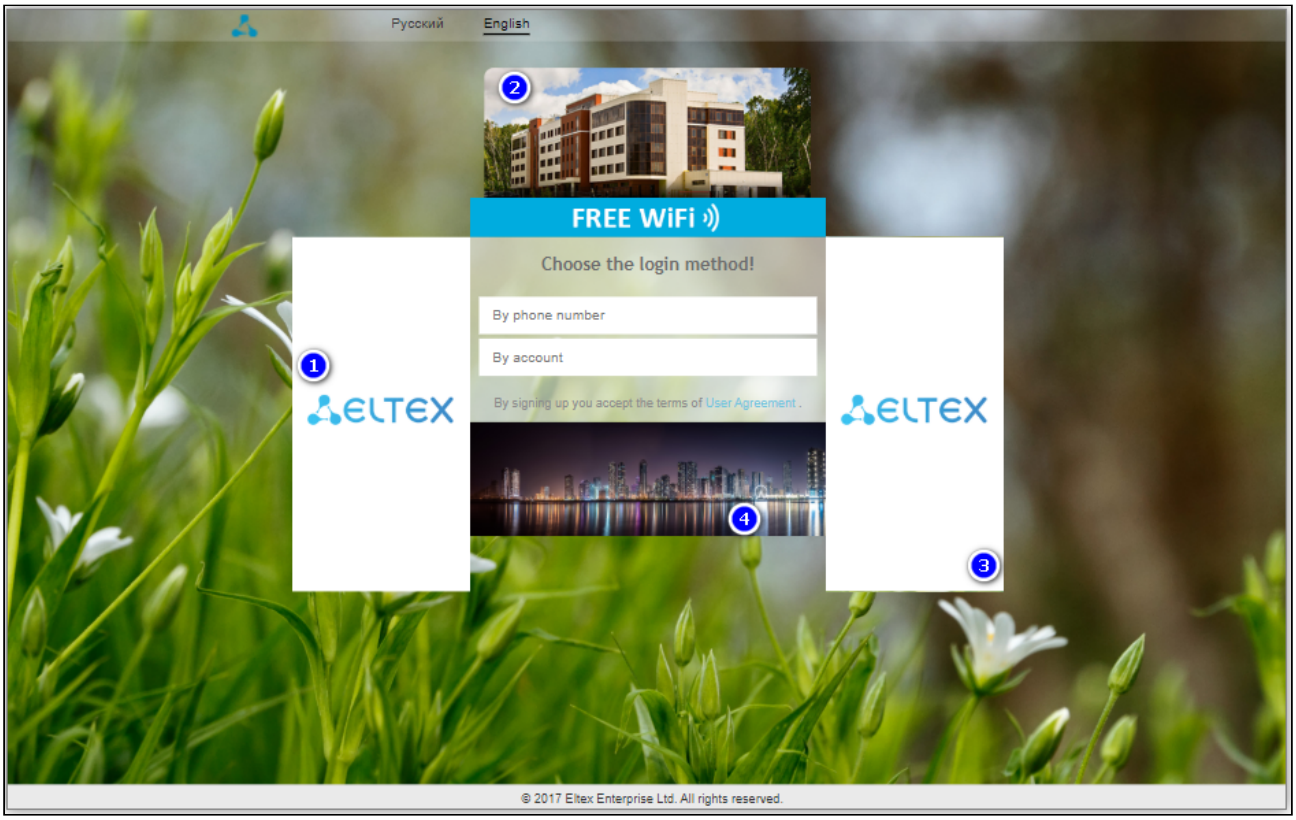



To select a new image or edit an existing one, the icon  is used. When it is clicked, a window for selecting an image from a gallery will be opened.

## Sections

### Common





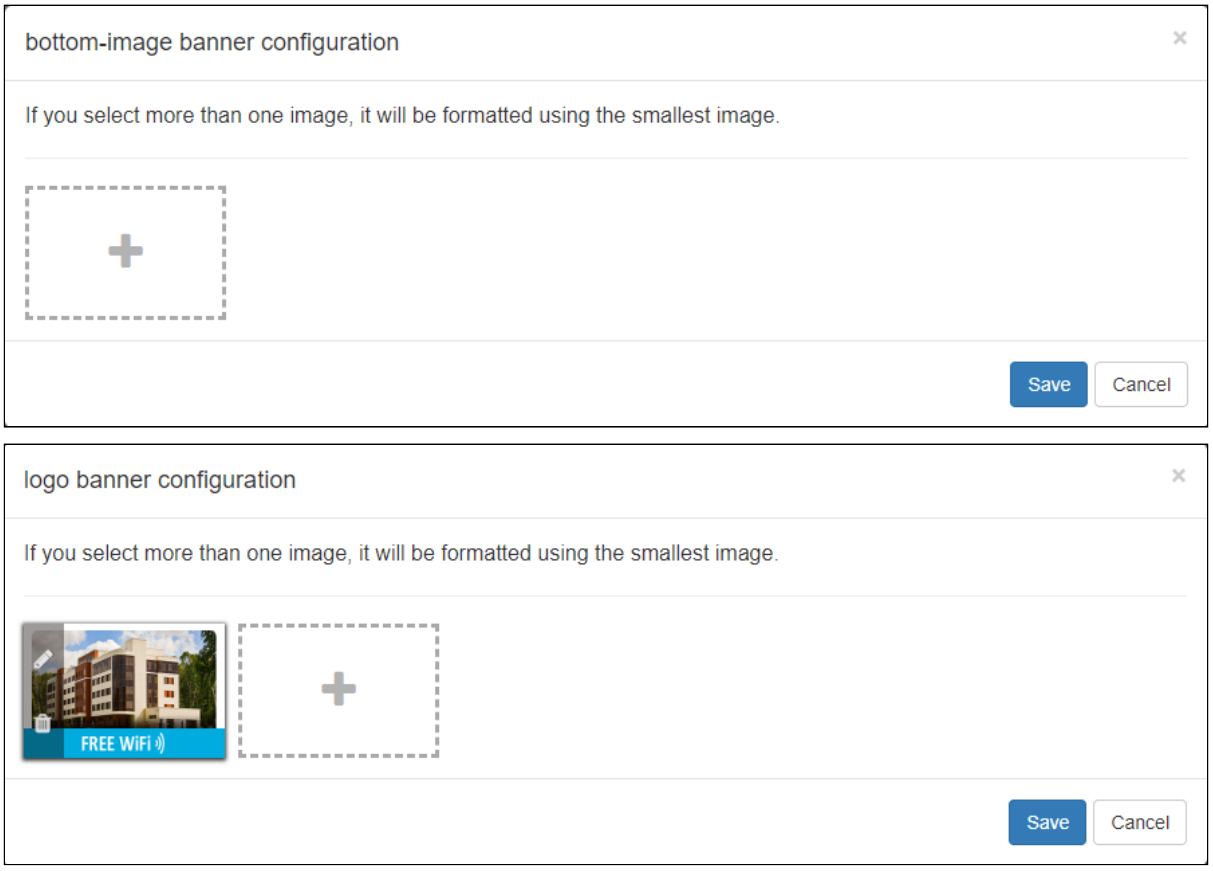

In this section the following parameters are configured:

- Icon (favicon) — an icon displayed in a page header in a user's browser. This icon will also be used when a portal will be displayed in the Portal Constructor. To change an icon, click its preview. A gallery will be opened to select another image.
- Page background — a background image of a portal page.
- Header background — a top panel with a logo and language selection.
- Top banner — is located above the user menu (2).
- Left banner — is located on the left from the user menu (1). Not displayed in the mobile version. Displayed in the tablet version only if the right banner is disabled.
- Right banner — is located on the right from the user menu (3). Not displayed in the mobile version. Displayed in the tablet version only if the right banner is disabled.
- Bottom banner — is located under the user menu (4).

It is recommended to use images with transparent background as they will blend in a portal's design.

GIF images displaying animation can be used as banner or background images, for example:

Configuring banners



To add a new banner or to edit an existing one, click the icon  near a banner's name (top, left, right, bottom, final). Added banners are displayed on a preview. To edit them, move the mouse pointer over a banner and click the icon  .

When a new banner is added, the button  is used to open a gallery for image selection. A banner may contain several images. In such configuration, they will replace each other. Change of images on all portal banners will be synchronized. Images displayed in one banner should have the same width and height (in pixels).

To change a selected image, click the icon  . To delete it, click  .

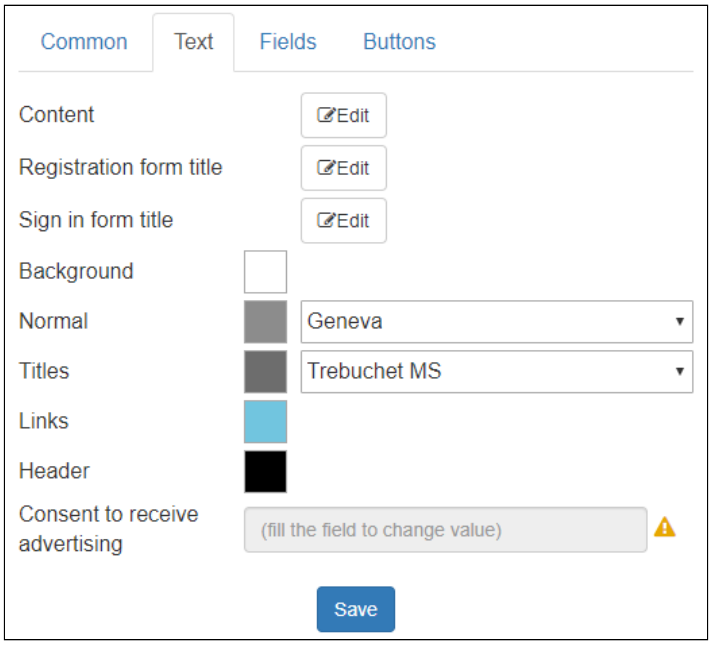
The system offers to configure banners for the shedule "Default". Another schedule created in the schedule configuration section can be selected before banner editing. When such a schedule is selected, it will be linked to a portal. Only banners configured for it will be displayed during working hours.

Thus, if a schedule is selected only for one banner, other banners will not be displayed according to this schedule.

When required images are selected, click "Save".

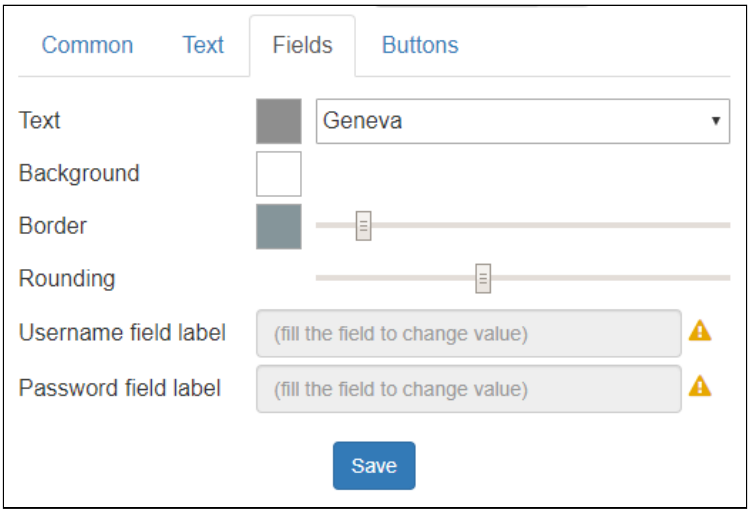
Remember that images should be the same size. For example, if the size of the first image in "Logo banner configuration" is 400px * 200px, the second and subsequent ones should have the same size (400px * 200px).

Text




- **Content** — a text displayed on a user registration page. Specified via a standard text editing form.
- **Registration form title** — a registration page title that will be displayed in a browser.
- **Sign in form title** — a sign in page title that will be displayed in a browser.
- **Background** — a background colour for the area containing text and control elements.
- **Normal** — a colour and a font used to display the main text on a portal.
- **Titles** — a colour and a font used to display page titles.
- **Links** — a colour of links (the font of the main text is used).
- **Header** — a colour used to display available languages in a header.

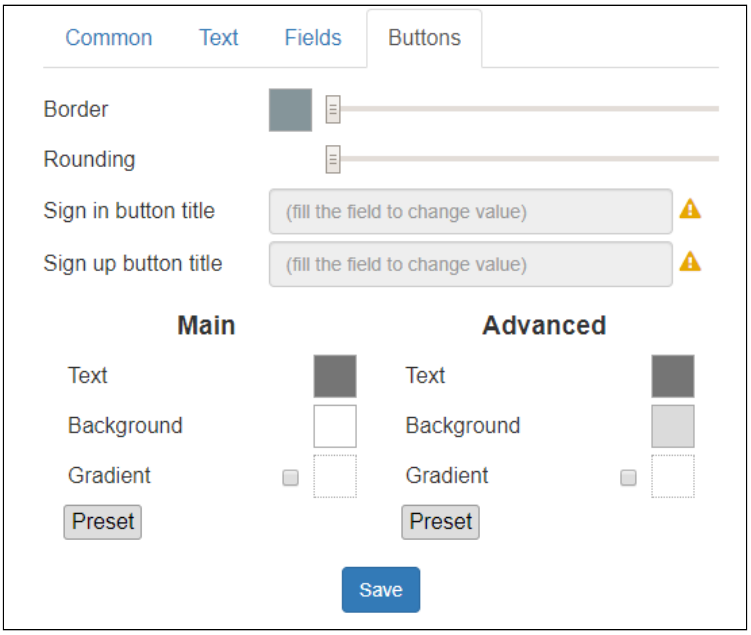
## Fields




- **Text** — a colour and a font of text fields.

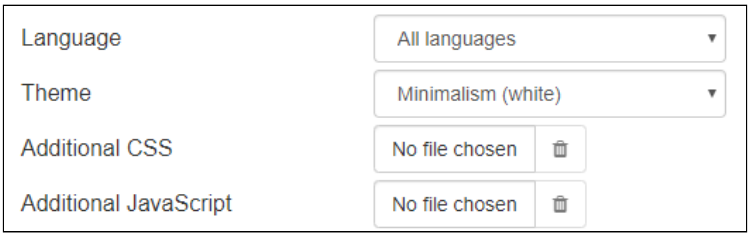
- **Background** — a background colour of text fields.
- **Border** — a colour and a width of a border.
- **Rounding** — a corner rounding radius of text fields.
- **Username field label** — a label displayed near a field with a username. The parameter can be changed only if a language for editing is selected.
- **Password field label** — a label displayed near a field with a password. The parameter can be changed only if a language for editing is selected.

## Buttons




- **Border** — a colour and a width of a button border.
- **Rounding** — a corner rounding radius of buttons.
- **Sign in button title** — a text displayed on a button for signing in with an existing user account.
- **Sign up button title** — a text displayed on a button for signing up with a new user account.
- **Text** — a button text colour.
- **Background** — a button colour.
- **Gradient** — creates a gradient fill on a button (if enabled).
- **Preset** — select pre-configured colour adjustments for buttons.

## Additional CSS




An option for uploadingfiles to a virtual portal for changing display settings of virtual portal elements. The option allows configuring portal elements for which GUI configuration cannot be implemented.

To cancel changes made after applying a css file, upload an empty one.

## v1.14_Requirements to portal graphic resources (EN)

### Header image (logo)

Height limitation is 24px. If an image size is larger, it is proportionally reduced (height and width). There are no limitations for an image width. If it is greater than a screen width, a horizontal scroll will be available. Thus, the width 260px and less is recommended (the width of IPhone 4 minus 60px for the language selection element).

### Top image (banner)

The image width itself is not clearly limited, but as it is located inside the main 400px block containing control elements, it should be not more than 400 px too. . If the image width is more than 400px, it is proportionally reduced. The height is not clearly limited. The higher the image, the lower is the location of control elements.

> If a screen width is less than 400px, the image will occupy all available width.

### Bottom image (banner)

The image width itself is not clearly limited, but as it is located inside the main 400px block containing control elements, it should be not more than 400 px too. If the image width is more than 400px, it is proportionally reduced. Height is not clearly limited. The higher the image, the higher the initial page.

> If a screen width is less than 400px, the image will occupy all available width.

### Right and left images (banners)

The banners have the top margin consistent with the top banner's bottom (i.e. 47px + top_image_height px). Maximum width is 200px, height is not clearly limited. The higher the image, the higher the initial page. If the image width is more than 200px, it is proportionally reduced. Image blocks border on the main block containing control elements. If the image width is less than 200px, it will be placed in a centre of a 200px block, and a space will seem to appear between the image and the main block.

> If both the right and the left banners are configured, and a screen width is from 600 to 800 px, the both banners are hidden. If either the right or the left banner is configured, the image is not hidden. If a screen width is less than 600px, images are hidden anyway.

### Background

A high-quality image is needed to be correctly displayed on big screens. An image should be centred in both X and Y directions and cover the whole background area (if an image is too small, it will be stretched that will result in a loss of background quality). It is not recommended to put significant elements on a background image, as when screen size is small (smartphones), it will be almost completely covered with control elements.

> Each image can be static (png, jpg) or dynamic (gif).

> Attention! Side banners are not displayed in mobile version.

### Information on other elements (buttons, labels, etc.)

The following elements can be configured:

- Icon (favicon) displayed in a browser
- Transparency and background colour of a header (a band on top of the screen containing a logo and elements for language selection)
- Page background. Can be filled with a colour or an image
- A text between a top banner and buttons for user identification scenario selection ("Welcome" or another text chosen by a designer can be displayed there)
- Background (colour, transparency) and font of the text from para.3 and of the phrase "By signing up you accept the terms of User Agreement"
- Text, fill colour and border colour of the fields for entering a phone number, a password and an accreditation number
- The labels "By account", "By phone number" on the corresponding buttons

- Labels located near the fields "Login", "Password" (for example, the word "Password" can be replaced with "Accreditation number")
- Colour and text of the buttons for scenario selection: identification by phone number or logging in using an accreditation number
- Colour and content of labels located near the input fields (pnone number, last name, password, accreditation number)
- Each banner can be enabled or disabled (not be displayed)

Elements order, banners location and the relative size of buttons are constant. Only one copy of each banner can be created. Thus, two top or bottom banners cannot be created.

### Additional pages

In addition to the login page, other pages can be configured on the portal:

- Enter SMS code (optionally)
- Success (text: "Success, you are connected to the Internet")
- Welcome (the text is: "Is 12345 your number?") — an optional page. If a session storage period is long, a user will not see this page
- Session end (text on exceeding a traffic or time limit) — an optional page. If unlimited tariffs are used, a user will not see this page
- User agreement (a user will be redirected to this page after clicking a corresponding link)
- Access denied (an attempt to address resources prohibited by a current service or a session processing scenario)
- Session expired (a user will see this page if opens a portal and does not input any data for more than five minutes)

Configured colour schemes for input elements (fields, buttons) will be displayed the same way for all pages. Configured graphical elements: logo, background and banners will be displayed the same way for all pages.

### Language settings

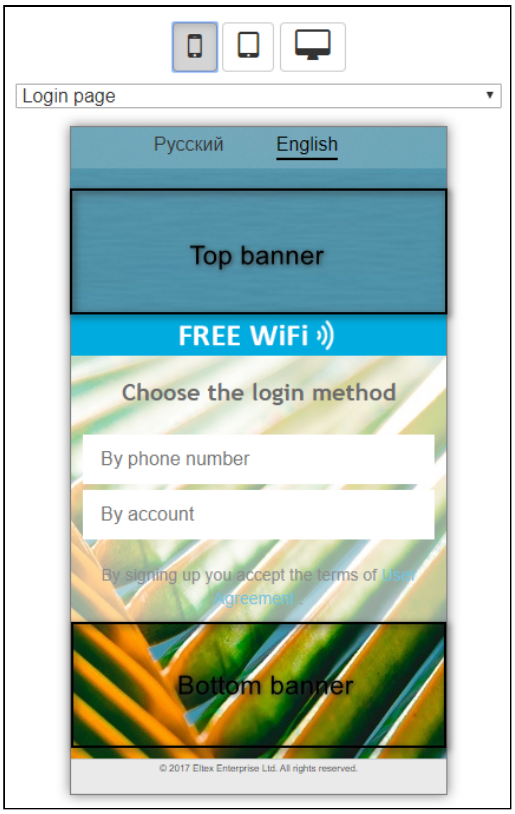
When a multi-language configuration is used, text labels and banners can be created separately for each language.
The languages supported by the platform:

- Russian
- English
- Chinese
- Kazakh

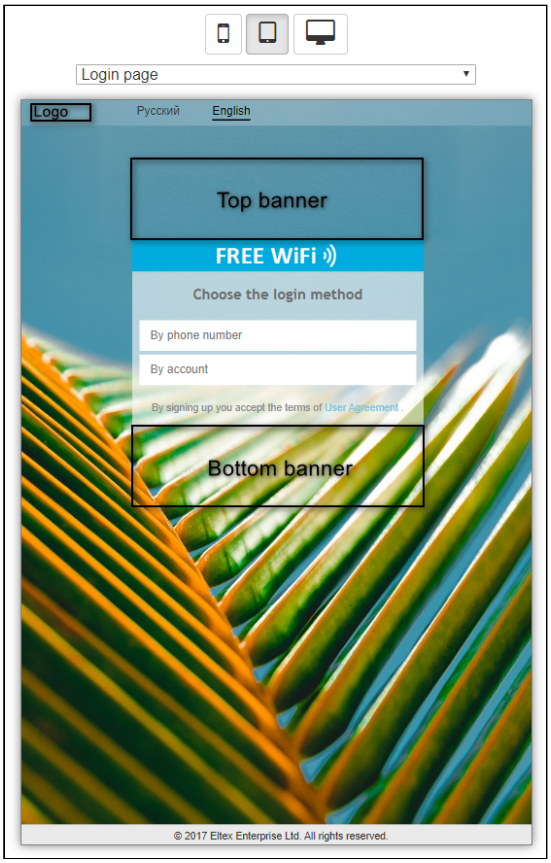
A colour scheme (buttons and fields settings) will be the same for all languages.

A layout of banners on a portal

Banners in the mobile layout:




Banners in the tablet layout:




Banners in the desktop (laptop) layout:

Banners in the desktop (laptop) layout when a user identification scenario is selected:


## v1.14_MAC Checker (EN)

MAC Checker is a service that provides REST-based API that allows getting an OTT access point's status by its MAC address on SoftWLC server.
An OTT access point can be in the following states:

| State | Description | What must have happened |
|---|---|---|
| **No MAC detected** | MAC address unknown | Either requests have not got from an access point to the Service Activator or something is wrong with a certificate or with the access point's firmware. Or that is not an OTT point. The Service Activator logs should be checked |
| **No init link** | AP in a sandbox | The Service Activator has successfully got requests from the access point, but there is no init link for the AP in SoftWLC, and the "ott_default" link is not created (see documentation on OTT) |
| **No OTT link** | OTT link does not exist | There is no OTT ESR with OTT profile in the domain specified in the init link |
| **Default Domain** | an AP is in a domain included into the default list | An AP has been successfully initialized and got into a domain which is specified as a default one in MAC Checker configuration |
| **Region Domain** | an AP is in a domain that is not included into the default list | An AP has been successfully initialized and got into a domain which is not specified as a default one in MAC Checker configuration |

MAC Checker should be started on a separate server that is accessible from the Internet (it has a public IP address or a traversed port).

By default, the service uses port 8088. The service accepts client's requests for MAC address check, sends relevant requests to the core via EMS NBI, gets the response from the core and generates a JSON response for the client. A response contains current *time*, normalized *MAC address*, *affiliation status*, *domain name* and an*error* occurred during processing.

The service should have IP connectivity to the EMS service via port 8080.

The module is configured via `/etc/eltex-ott-mac-checker/application.conf`. Event log is located in `/var/log/eltex-ott-mac-checker`.

Example of a request to the service using curl utility:
*curl -g http://192.168.42.197:8088/ottChecker/checkMac?mac=a8:f9:4b:22:22:22 --header "Accept: application/json"*
Response:
*{"time":1536304889422,"macAddress":"a8:f9:4b:22:22:22","status":"No MAC detected","information":null,"error":{"code":null,"description":null}}*

## Service installation

*apt-get install eltex-ott-mac-checker*

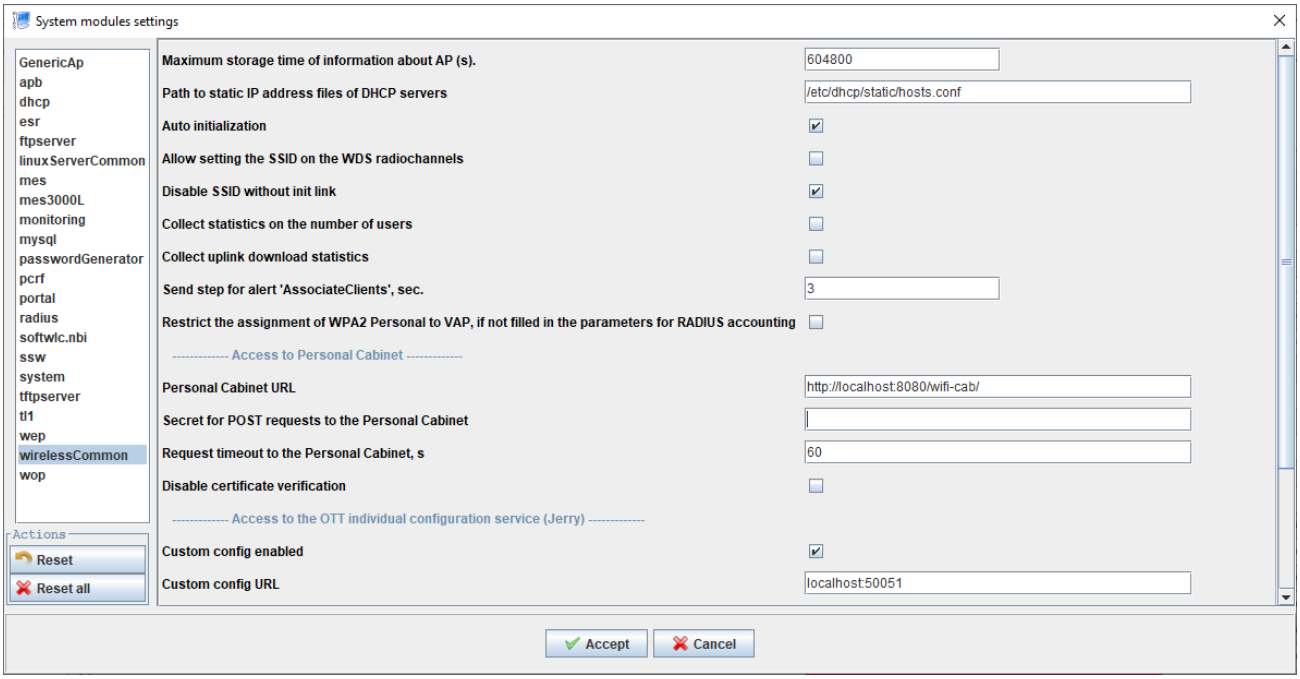
### v1.14_Jerry (EN)

The service is a JAVA-based API. It allows managing OTT individual configurations for ESR-10 — creating, editing, initialization binding.

The service can be started on a separate server. JAVA 8 is required. By default, the service uses port 50051.

The configuration file is located in `/etc/eltex-jerry/application.conf`. MongoDB connection, the address and the port on which the service works are configured there.
Logs are located in `/var/log/eltex-jerry/main.log file`.

On EMS side, select "Administration" → "EMS server configuration" → "System modules" → "Wireless common":




Configure connection in the section "Access to the OTT individual configuration service (Jerry)".

Service installation: `apt-get install eltex-jerry`
It is recommended to install Jerry on the same server as EMS.

## v1.14_Mercury (EN)

Mercury is a service for Hotspot users' accounts management (it is used by eltex-portal and eltex-apb services).

Interaction between services is based on gRPC API.

Service configuration files:

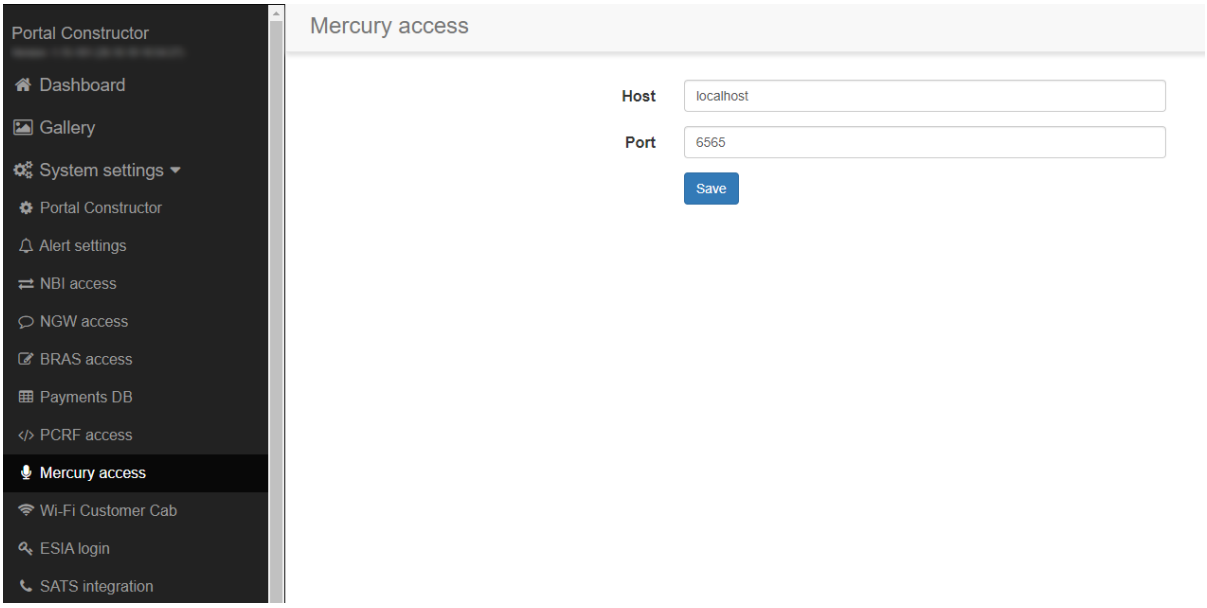
- */etc/eltex-mercury/application.conf*

```
database {
  host = localhost
  port = 3306
  name = radius
  user = javauser
  password = javapassword

  readOnly = false           # For ReadOnly database

  pool {
    maxPoolSize = 20         # Maximum number of database connections
    minimumIdle = 1          # Minimum number of idle connections
    connectionTimeout = 5000 # Database connection timeout
  }

}

# Enable sending information on changes in radstat table to logging-service
sorm3Enabled = false

# Configuring connection to eltex-logging-service
logging {
    host = localhost
    port = 9099
}
```

- */etc/default/eltex-mercury*

```
# Eltex-Mercury daemon parameters

# Initial size of Java heap
JAVA_INIT_HEAP=16m
# Maximum size of Java heap
JAVA_MAX_HEAP=256m

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-mercury"

PORT=6565
```

Communication between **eltex-portal** and Mercury is set in Portal Constructor — "System settings" - "Mercury access":




Communication between **eltex-apb** and Mercury is set in apb configuration file - */etc/eltex-apb/apb.properties*:

```
...
mercury.host=localhost
mercury.port=6565
mercury.pool.size=100
...
```

Service installation: *apt-get install eltex-mercury*

## v1.14_Bob (EN)

- Service description
- Settings

### Service description

Eltex-Bob is a RESTful API service intended for unloading AP information into a monitoring system in JSON format. By default, the service can be requested via port 9190 using a GET request.To get information on a number and a state of devices, an access to MySQL is required.To provide protection from DDoS attacks, the service has its own cache that makes it possible not to load a database. The service requests an AP list every hour. Information on accessibility of devices is updated every minute. Available API methods:

- http://<<ip_address>>:<<port>>/GetAPList - AP list in JSON format
- http://<<ip_address>>:<<port>>/GetAPDetail/{MAC_ADDRESS} - Detailed information on AP
- http://<<ip_address>>:<<port>>/GetAPAvailable/{MAC_ADDRESS} - AP availability
- http://<<ip_address>>:<<port>>/GetAPPerformance/{MAC_ADDRESS} - AP performance metrics

**GetAPList** provides an AP list in JSON format that contains:

APHOSTNAME - device MAC address;

APVISIBLENAME - device name;

APGROUP - AP location specified according to a reference table;

APRTCGROUP - a domain in which a device is located (except for a hidden part - domain_search.regex, see Service settings);

FULLADDRESS - a column of a reference table that contains an AP location address.

Example:


```
{
    "data": [
        {
            "{#APHOSTNAME}": "a8:f9:4b:b4:99:60",
            "{#APVISIBLENAME}": "WEP-12ac",
            "{#APGROUP}": "Baikal Bank/Sakha (Yakutia)/Subsidiary office №178-758",
            "{#APRTCGROUP}": "Dalniy_Vostok/Habarovskiy_filial/Evreyskaya_AO/Obluche/Sberbank/
4157-081_Kuznechnaya_11a",
            "{#FULLADDRESS}": "678100, Olyokminsk, Molodyozhnaya Street, 20741"
        },
    ]
}
```


**GetAPDetail** Detailed information on an AP that contains:

"ip" - device IP address

"office" - a value for a VSP selected from a reference table

"city" - a value for a VSP selected from a reference table

"firmware-version" - firmware version

"serial-number" - device serial number

"vsp" - a value for a VSP selected from a reference table

"full-address" - a value for a VSP selected from a reference table

Example:

```
{
    "ip": "192.168.6.18",
    "office": "Subsidiary office №178-758",
    "city": "Beryozovsky",
    "firmware-version": "1.16.0.163",
    "serial-number": "WP01000177",
    "vsp": "4157-081"
    "full-address": "678100, Olyokminsk, Molodyozhnaya Street, 20741"
}
```

**GetAPAvailable** AP availability that contains:

"available" - AP availability, where 0 - AP is available, 1 - AP is unavailable

"uptime" - AP availability duration in seconds

Example:

```
{
    "available": 0,
    "uptime": 67370
}
```

**GetAPPerformance** AP metrics that contain:

"wifi_users" - number of connected users

Example:

```
{
    "wifi_users": "5"
}
```

Service authorization can be performed in two ways:

- http-basic authorization that is enabled in service settings
- An ACL list specified in nginx configuration file

## Settings

To restrict the number of IP addresses that can access the service, configure nginx server using ACL. An Access Control List is added to nginx configuration file, for example:

where deny - IP address from which access is restricted

allow - IP address from which access is allowed

in the example below, access is restricted for all IP addresses but 192.168.1.3 and 127.0.0.1.

```
location /api {
    allow 192.168.1.3/24;
    allow 127.0.0.1;
    deny all;
}
```

If to access Bob nginx is used, configure proxying

```
server {
    listen 80;
    server_name bob;
    location /api/ {
        proxy_pass http://localhost:9190/;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_redirect default;
    }
}
```

Service configuration:
The main configuration file is located in `/etc/eltex-bob/application.properties`:

```
# The Datasource Mysql properties
spring.application.name=bob
#An address of a server with MySQL database from EMS
spring.datasource.url=jdbc:mysql://localhost:3306/eltex_ems?
useSSL=false&useJDBCCompliantTimezoneShift=true&useLegacyDatetimeCode=false&serverTimezone=UTC
spring.datasource.username=javauser
spring.datasource.password=javapassword

# Common properties
#domain_search.mask=%
domain_search.mask=%.ap.root - the domain used for unloading. Includes subdomains

domain_search.regex=^root/Ap/(.*)$  - a domain part that will be hidden while displaying a result
domain_search.replacement=$1

mac.splitter=: - delimiters for MAC address octets (":" by default)


auth.enabled=true - enabling login-password authorization, false - disabled
auth.username=eltex - login for authorization on Bob service
auth.password=eltexeltex - password for for authorization on Bob service

excel.config.file=/etc/eltex-bob/excel_config.yaml - configuration file to maintain a VCP
reference table.

server.port=9190 - a port listened by the service
```

Configuration file for working with a reference table - /etc/eltex-bob/excel_config.yam:

```
vspSheetName: For tenders - Name of a page for analysis
vspExcelFile: /home/vagrant/list2.xlsx - file path

type: TITLE - defines a mode for using the table. TITLE - columns will be searched by their
titles, NUMBER - columns will be searched by their sequence number 0,1,...
columns:
  vsp: VSP number - in this column, a cell with VSP number consistent with one from a domain is
searched. For example, "4157-081" for the domain .../Sberbank/4157-081_Kuznechnaya_11a...
  bank: Regional bank           \
  region: RF territorial entity                  - cells from these columns will be used to make
an APGROUP
  office: Office name           /
  address: Real address - values contained in this cell get into FULLADDRESS in GetAPList output

## Configuration example by column numbers
#vspSheetName: For tenders
#type: NUMBER
#columns:
#  vsp: 3
#  bank: 1
#  region: 10
#  office: 2
#  address: 7
```

By default, the service uses 10 connections to a database. This number can be increased when necessary by adding the following line *spring.datasource.hikari.maximum-pool-size=20* (where 20 is the number of connections) to the configuration file.

A service initialization file is located at: `/etc/default/eltex-bob`.

## v1.14_Disconnect (EN)


- Service description
- Description of work
- Configuration


### Service description

A microservice intended for session deauthentication and user MAC address removing. Eltex-disconnect interacts with the PCRF service to directly send a user session removing command and with the Doors authentication service to validate incoming JWT tokens.

Available API methods: **`disconnect`**

- Eltex-disconnect will provide the following response in success:

```
{
    "success" : true
}
```

- If an error occurs, a response will be as follows:

```
{
    "success" : false,
    "fail" : "description of the error occured"
}
```

## Description of work

Disconnect waits for a GET request on port 9096 `http://\{\{Ip_address\}\}:9096/disconnect?token=\{\{token\}`
Request example:

```
http://192.168.49.110:9096/disconnect?
token=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ1c2VyIiwiYXV0aCI6WyJST0xFX0FETUlOIl0sImlhdCI6MTU1OTI3OTU4MCwiZXhwIjoxNTU5MzUxNTgwLCJuYXNJcCI6IjEwMC4xMTIuMC4xIiwic2Vzc2lvbklkIjoiNTY5MjU0OTkyODk5NjMwNzk2NCIsInZyZiI6IjEiLCJjbGllbnRNYWMiOiJGQy00NS05Ni01Ri01MC1BQyJ9.fWhOkgFo_rLd2mB9_70HotPH9LlGh7SuT1-qDQvv77U
```

After receiving a GET request, eltex-disconnect sends an obtained token to eltex-doors in order to check if data has been really sent from an authorized source. Eltex-doors checks a token and gives a response depending upon whether it is valid or not.

The next step is decoding of a token from which payload (metadata) on a session of a user to be deauthenticated is extracted.

Decoded token example:

```
{
  "sub": "user",
  "auth": [
    "ROLE_ADMIN"
  ],
  "iat": 1559279580,
  "exp": 1559351580,
  "nasIp": "100.112.0.1",
  "sessionId": "5692549928996307964",
  "vrf": "1",
  "clientMac": "FC-45-96-5F-50-AC"
}
```

Description of the payload token fields

```
sub - a user
iat - token creation time
exp - token lifetime
nasIp - device's nas
sessionId - unique user session
vrf - Virtual Routing and Forwarding
clientMac - client's MAC address
```

A disconnect GET request including all necessary parameters is sent to API PCRF: VRF, Mac, sessionId, nasIp

Request example:

```
GET http://127.0.0.1:7070/account/disconnect?
session=5692549928996307974&nas_ip=100.112.0.1&vrf=1&single=false&mac=FC-45-96-5F-50-
AC&remove_mac=true
```

PCRF performs appropriate actions: deauthentication and MACC address removing.

## Configuration

The service's configuration file is located at `/etc/eltex-disconnect-service/application.conf`

```
pcrf {
  host = localhost            PCRF service address
  port = 7070                the port listened by PCRF
  timeout = 100                response timeout
}

doors {
  host = localhost            address of Doors service
  port = 9097                port listened by Doors
  path = /api                path to request Doors
  timeout = 200                response timeout
  connectionTotal = 100        maximum number of connections to Doors
}
```

The logging configuration file `/etc/eltex-disconnect-service/log4j2.xml`

The configuration file for service initialization `/etc/default/eltex-disconnect-service`

```
PORT=9096                          The port listened by the service

# Initial size of Java heap
JAVA_INIT_HEAP=4m                RAM size allocated during initialization
# Maximum size of Java heap
JAVA_MAX_HEAP=32m                 RAM size allocated during operation

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-
disconnect-service
```

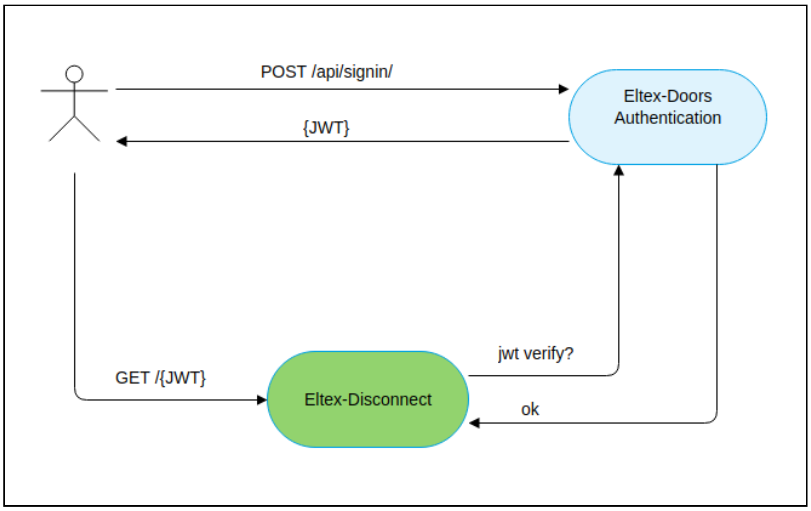
## v1.14_Doors (EN)


- Description
- Configuration


### Description

Eltex-doors is a service that provides user authentication by creating a token and verifying it.

Eltex-doors forms a JWT token based on a POST request and containing login, password and metadata.




JWT(JSON Web Token) - a JSON object defined in RFC 7519

Generated tokens are keeped in the `auth_token` table of the `eltex-doors` database. On expiry of the period specified in the configuration file (token.expire.timeout), outdated tokens are deleted from the database.

The parameters "token lifetime{iat}" and "token creation time{exp}" are specified in a token's payload and can be obtained by token decoding.

Available API methods: `/api/signin/`

An example of parameters sent in a POST request

```
{
    "username": "user",
    "password": "password",
    "metadata": {
        "nasIp": "100.112.0.1",
        "sessionId": "56925499289963086 67",
        "vrf": "1",
        "clientMac": "FC-45-96-5F-50-AC"
    }
}
```

- In success, the service's response will be:

```
{
    "status": "OK",
    "accessToken":
"eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ1c2VyIiwiYXV0aCI6WyJST0xFX0FETUlOIl0sImlhdCI6MTU1OTcwOTQ2OCwiZXh
wIjoxNTU5NzgxNDY4LCJuYXNJcCI6IjEwMC4xMTIuMC4xIiwic2Vzc2lvbklkIjoiNTY5MjU0OTkyODk5NjMwODY2NyIsInZy
ZiI6IjEiLCJjbGllbnRNYWMiOiJGQy00NS05Ni01Ri01MC1BQyJ9.VQ1NKCcG445eSMz7jOoTGt7PC1HVhTkFxxwWWxdVO3Y"
}
```


where `status` - response status

access `token` - generated token

- If an error occurs, the service will answer:


```
{"status":"FAIL","error":"Invalid username or password"}
```


where `status` - response status

`error` - error description

## Configuration

The configuration file is located at `/etc/eltex-doors/application.properties`

```
## Mysql datasource properties
spring.datasource.url=jdbc:mysql://<<ip_address>>:3306/eltex_doors?
useSSL=false&useJDBCCompliantTimezoneShift=true&useLegacyDatetimeCode=false&serverTimezone=UTC
spring.datasource.username=eltexdoors           Login
spring.datasource.password=eltexpassword        Password

spring.flyway.url=jdbc:mysql://localhost:3306/eltex_doors?
useSSL=false&useJDBCCompliantTimezoneShift=true&useLegacyDatetimeCode=false&serverTimezone=UTC
spring.flyway.user=eltexdoors                   Login
spring.flyway.password=eltexpassword            Password

## Eureka settings and starting server port
server.port=9097                                The port listened by the service

## Custom application properties
## Token expiration timeout
# Use time format HH:mm:ss
auth.cron.session.timeout=*/60 * * * * *        Token lifetime checking period
auth.token.expire.timeout=20:00:00              Token lifetime

# Login and password from basic account
auth.username=user                              A login to connect to eltex-doors
auth.password=password                          A password to connect to eltex-doors
```

The logging configuration file `/etc/eltex-doors/log4j2.xml`

The configuration file for service initialization `/etc/default/eltex-doors`

```
# AP Monitoring service

# Initial size of Java heap
JAVA_INIT_HEAP=8m                           Amount of RAM allocated during initialization
# Maximum size of Java heap
JAVA_MAX_HEAP=64m                           Amount of RAM allocated during operation

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-doors"
```

## v1.14_Logging (EN)

Logging-service is a service that provides logging of information on portal users accounts (is so far used for the service eltex-mercury).

Interservice exchange is based on `gRPC API`.
Logging-service interacts with the database `wifi-customer-cab` and writes received data to the `eventlog` collection (the table "Event log - Wi-Fi users event log" in the Admin Panel GUI).

Service configuration files:

- `/etc/eltex-logging-service/application.conf`

```
# A port on which the service operates
server {
  port = 9099
}

# Adding an entry to the eventlog collection
eventlog {
  enabled = true
}

# Enable sending data to SORM
# The functionality is under development
sorm {
  enabled = false
  dir = /var/log/eltex-logging-service/sorm3/
}

# Configuring access to an Admin Panel database
database {
  uri = "mongodb://localhost:27017/wifi-customer-cab"
  poolSize = 5
  timeout = 5s
}
```

- `/etc/default/eltex-logging-service`

```
# Initial size of Java heap
JAVA_INIT_HEAP=4m
# Maximum size of Java heap
JAVA_MAX_HEAP=32m

# Additional arguments to pass to java
JAVA_OPTS="-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/log/eltex-logging-service"
```

Service installation: *apt-get install eltex-logging-service*

## v1.14_WIDS (EN)


- Licensing
- Enabling the service on APs
- Service configuration on access points and low-level logic
- eltex-wids-service configuration


WIPS/WIDS is an access point (AP) internal service that detects and prevents wireless intrusion.

This mechanism monitors the AP radio spectrum for the presence of security risks, alerts the system administrator whenever a threat is detected and takes countermeasures if necessary.

In the current version (1.17.0), the following functionality is available:

1. DDoS attack detection;
2. Brute force attack detection;
3. Mis-configured AP detection;
4. SSID-spoofing AP detection;
5. MAC-spoofing AP detection;
6. Client disconnection from rogue APs.

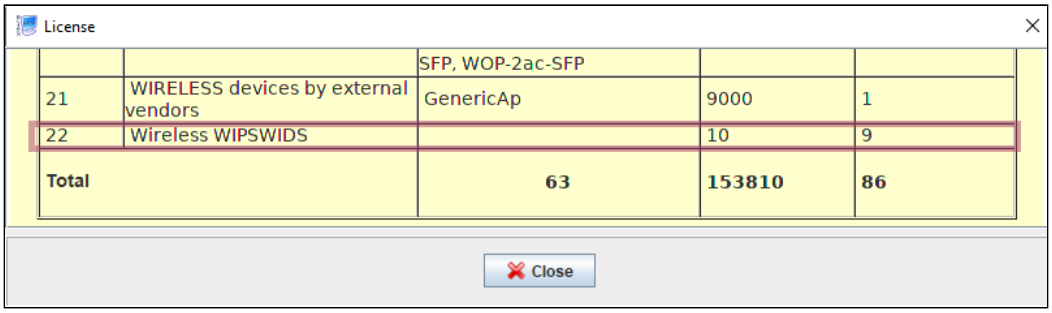
**eltex-wids-service** — an external service on the server side that distributes white/black lists of "rogue" APs between WIPS/WIDS.

## Licensing

The license restricts the WIPS/WIDS service configuration and monitoring in the Management system.

The service can be enabled on 2 APs under the demo (default) license.

The number of available and applied licenses can be found in *Help - Licenses* section of GUI EMS or directly in */usr/lib/eltex-ems/conf/licence/licence.xml* license file.




**/usr/lib/eltex-ems/conf/licence/licence-dist.xml**

```
<group>
    <title>Wireless WIPSWIDS</title>
    <count>10</count>
    <typeList>
        <type>WiFi</type>
    </typeList>
</group>
```

If the license for WIPS/WIDS is in the list, the *"WIDS manager"* tab will be available in the *"Wireless"* menu of GUI EMS:

Relevant checkboxes will be available in the *"Access"* tab of an APs' menu.

## Enabling the service on APs

The AP to which the license can be applied is explicitly defined in GUI EMS. In the "Access" tab, the following two settings can be found:

- The "On WIPS/WIDS service" parameter that defines the AP that will use the service. Once the checkbox is set, the number of available licenses will be one less. By default, the checkbox is not set, which means that WIPS/WIDS service is not available.
- The "Really used WIPS/WIDS" parameter is a non-editable checkbox that shows if the system has enabled the service. It may happen that the "On WIPS/WIDS service" checkbox is set for more APs that are permitted under the license — then the checkbox will be deselected for some APs, although the "On WIPS/WIDS service" checkbox is set.

If the service has been enabled successfully, that is, both checkboxes are set in the "*Access*", then:

- the new section "*WIDS/WIPS*" will appear in the "*Configuration*" tab

- events related to WIDS/WIPS service will be displayed in "*Events log*" and "*Active alerts*" sections of the "*Monitoring*" tab

## Service configuration on access points and low-level logic

All access points in a spectrum can be divided into three groups:

- "untrusted" APs — access points that are in a spectrum, but nothing is known about them;
- "trusted" APs — access points that are installed and managed by an operator;
- "rogue" APs — access points that definitely threaten the network (spoof MAC address or SSID of original APs).

To identify all "untrusted" access points in a spectrum explicitly, a dynamically changed encrypted entry is added to the Beacon packet of the AP that uses WIDS.
Only those access points that have the same *Shared key* in service configuration can decrypt the packet. If the entry is missing, or if the result is not as expected initially, the access point will be considered as "untrusted" one. Otherwise, as "trusted" one.
If an "untrusted" AP has the same MAC address or SSID as a scanning AP has, it will be considered as "rogue", and a relevant trap will be sent to the Management system.

**Trap example**

```
Дата создания              : 2019-05-13 15:31:04
Название источника         : WEP-12ac_13
Сообщение                  : Rogue AP detected with MAC address: E0:D9:E3:4F:9D:F0, ssid Eltex-
Local, channel 1!
Приоритет                  : CRITICAL
OID                        : 1.3.6.1.4.1.35265.1.60.1.8.3.0.2
```

For the service to operate more flexibly, the list of access points that should or should not be considered as "trusted" can be specified. The list is disseminated between access points by the supporting service — *eltex-wids-service*.

Most *eltex-wids-service* configuration is done in "*WIDS/WIPS"* tab of "*Configuration"* menu

| **Parameter** | **Values** | **Description** |
|---|---|---|
| | | WIDS Parameters |
| Status | Down/Full/Key-only | Down - disable the service (default value).<br>Full - enable the attack detecting service.<br>Key-only - enable the service, but disable threat detection.<br>In the "Key-only" mode, an AP will add an encrypted entry to Beacon packets to be included into "trusted" AP lists of opposite APs, but it will not detect threats on its own. In this mode, only the *Shared key* field is available. |
| Shared key | ASCII string of length from 10 to 32 | A shared key used for detecting trusted APs in a spectrum.<br>By default, it is not specified. The service will not be enabled until Shared key is specified. |
| WIDS list URL | ws://<ip>:<port>/MacLists | The path to eltex-wids-service.<br>Optional setting. |
| WIDS MAC list | The name of MAC address list | The opportunity to choose one of the MAC address lists created in *"Wireless - WIDS Manager"* is provided.<br>Optional setting. |
| Scan mode | Passive/Sentry | Spectrum scanning mode.<br>Passive - in this mode, an AP will change its current channel (where client services are implemented) to another channel from the list for short time intervals (*Passive scan duration*) over certain periods of time (*Passive scan interval*) in order to detect other APs in a spectrum (default value).<br>Sentry - scan mode. Interaction between an AP and clients is not intended. An AP is constantly scanning the channel list and detects threats as quickly as possible. |

| | | |
|---|---|---|
| Passive scan interval, sec | 5..3600 | Passive scan interval (by default): 20 sec |
| Passive scan duration, ms | 10..2000 | Passive scan duration (by default): 100 ms |
| Prevention mode | None/Rogue/All | Threat prevention mode.<br>None - disabled (default value).<br>Rogue - a scanning AP detects MAC addresses of the clients connected to "rogue" APs and sends a DeAuth packet on behalf of the "rogue" AP to the client and vice versa.<br>All - in this mode, a forced DeAuth is sent to "rogue" APs, "untrusted" APs and clients connected to them. |
| DoS Detection Parameters | | |
| Mode | Up/Down | Down — DoS attack detection disabled (default value).<br>Up - DoS attack detection enabled.<br>If the limit of managing frames it the spectrum is exceeded, it is a DoS attack. Only the frames, destination MAC of which is the same as the address of a scanning AP are analysed (Beacon is an exception). |
| Interval, sec | 1..86400 | The interval during which frame counting is conducted. If during this time the specified limit is exceeded, the SNMP trap on attack detection will be generated.<br>Trap example<br>`Creation date : 08.07.2019 17:30:20`<br>`Название источника : WEP-12ac_13`<br>`Source : Denial of service" attack has been detected on wlan1 (5GHz): too many Beacon packets (counted 159 packets given the limit of 99). 40 attacks found during the last interval`<br>`Priority : CRITICAL`<br>`OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.1`<br>1 second by default |
| ... threshold | 1..10000 | Threshold for each type of management frames (Assoc, ReAssoc, DiAssoc, Auth, DeAuth, RTS, CTS, Prob, Beacon, BlockAck, BlockAckReq, Pspoll).<br>Default values:<br>• for Assoc, ReAssoc, DiAssoc, Auth, DeAuth - 50<br>• for RTS, CTS, Prob, BlockAck, BlockAckReq, Pspoll - 100<br>• for Beacon - 200 |
| Bruteforce Detection Parameters | | |

| | | |
|---|---|---|
| Interval, sec | 0..86400 | Brute force detection function.<br>During the interval, the number of unsuccessful authorizations on SSIDs with encryption (Personal and Enterprise) that are used by a scanning AP is counted. At exceeding of the Threshold, a brute force attack detection trap is sent to the Management system.<br>Trap example<br>`Creation date : 12.07.2019 14:37:02`<br>`Source : WEP-12ac_13`<br>`Message : Brute force attack detected on wlan0vap2(2.4GHz)(_ES_24_test_timers_enter), the last attempt was from the MAC address: 0c:9d:92:6e:d9:20`<br>`Priority : CRITICAL`<br>`OID : 1.3.6.1.4.1.35265.1.60.1.1.1.14`<br>Default value: 5 sec<br>If set to 0 - Brute force attack detection will be disabled. |
| Threshold | 1..10000 | Unsuccessful authorization threshold.<br>Default value: 25 |

If WIPS/WIDS service is enabled, an AP automatically sends traps to the Management system on each configuration change if the final configuration is unsafe.

**Trap example**

```
Creation date             : 01.07.2019 02:13:09
Source                    : wep12
Message                   : Unsafe configuration detected. System: Standard password; wids-service: Rogue AP attack prevented;
Priority                  : CRITICAL
OID                       : 1.3.6.1.4.1.35265.1.60.1.8.3.0.6
```

Criteria for unsafe configuration can be found here

## eltex-wids-service configuration

Redefinition of "trusted" and "rogue" APs is usually done by specifying the lists explicitly in "Wireless - WIDS Manager" section of GUI EMS and defining them in "*WIDS MAC list*" field in "*WIDS/WIPS*" tab of "AP*Configuration*" menu.

Service configuration file — */etc/eltex-wids-service/config.json*:

**/etc/eltex-wids-service/config.json**

```
{
  "ServicePort": 9095,
  "Database": "wids",
  "MongoConnectionString": "mongodb://localhost:27017",
  "FileLog": "/var/log/eltex-wids-service/log.log",
  "Environment": "production",
  "LogLevel": "debug",
  "MaxAge": 7,
  "MaxSize": 5,
  "MaxBackups": 14,
  "SleepDaemonQueueTime": 50000,
  "FoulTime": 60,
  "GelfHost": "lab3-test.eltex.loc:12201"
```

## v1.14_Unsafe configuration criteria

| Brief description of the problem | OID in the trap sent to the Management system | Assessment criteria | Detailed description |
|---|---|---|---|
| Default password | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.1 | Checking that "system->encrypted-password" is equal to a default value | Checking the password used to access the system |
| Shared key is not specified with WIDS enabled | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.14 | Checking that "wids-service->network-shared-key" is not empty | WIDS can not be used for detecting access points in a spectrum without the shared key specified. If the key is not specified, the service will not work. |
| Using a default ipsec password | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.8 | Checking that ipsec is enabled, and "ipsec->password" is equal to "password" | Using ipsec tunnel with a default password is considered to be unsafe |
| Using a default xuser ipsec | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.9 | Checking that ipsec is enabled, and "ipsec->xuser" is equal to "user" | Using ipsec tunnel with a default xuser is considered to be unsafe |
| Using a default xpassword ipsec | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.10 | Checking that ipsec is enabled, and "ipsec->xpassword" is equal to "password" | Using ipsec tunnel with a default xpassword is considered to be unsafe |
| Using unencrypted WGB | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.11 | Checking that the "security" parameter is set to "plain-text" for enabled WGB | Using wireless communication without data encryption is unsafe as it may lead to traffic interception or spoofing |

| | | | |
|---|---|---|---|
| Using unencrypted WDS | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.12 | Checking that "wds-security-policy" parameter is not equal to "wpa-personal" for enabled WDS | Using wireless communication without data encryption is unsafe as it may lead to traffic interception or spoofing |
| Using open VAP interface without authorization | 1.3.6.1.4.1.35265.1.60.1.8.3.1.9.13 | Checking that both wpa-personal/enterprise authorization and portal authorization are not configured for VAP interface | Using open networks without portal authorization contravenes the laws of the Russian Federation as it makes it impossible to identify a user. |

# v1.14_SoftWLC licenses and certificates (EN)


- EMS device licenses
  - Purpose
  - Licensing procedure and installation
  - Verification
- Admin Panel licenses
  - Purpose
  - Licensing procedure and installation
  - Verification
- PCRF licenses
  - Purpose
  - Licensing procedure and installation
  - Verification
- RADIUS certificates
  - Purpose
  - Licensing procedure and installation
  - Verification
- GUI EMS certificates
  - Purpose
  - Licensing procedure and installation
  - Verification


## EMS device licenses

### Purpose

The number of devices served by a program copy is limited by licenses for the devices.

### Licensing procedure and installation

A demo license including three devices of each type for a user to evaluate the system is integrated into EMS package by default.

Eltex specialists will generate a personal root license file in the acquisition of licenses. The file should be put into the following directory:

```
/usr/lib/eltex-ems/conf/licence/
```

the demo license file should be overwritten (or deleted in advance).

As the number of licenses increases, new files are added to the same directory without root file deletion. Device licenses are aggregated across all files.

When license files have been changed, restart eltex-ems process.

If any questions corresponding license and device acquisition occur, please, contact the managers of Eltex commercial department, phone: +7 383 274-10-01, e-mail: eltex@eltex-co.ru or order a call on our website: https://eltex-co.com

## Verification

To check if a license has been applied successfully, select "License" in "Help" tab of GUI EMS. Information on the current license and device restrictions will be available in the opened window.

| Number | Group | Devices | Restriction | Use devices |
|---|---|---|---|---|
| 1 | ACS server | | 1 | 0 |
| 2 | DHCP servers | DHCP | 2 | 0 |
| 3 | ESR devices | ESR-10, ESR-1700, ESR100, ESR1000, ESR1200, ESR200 | 1000 | 2 |
| 4 | MES Linux devices | MES3000L | 100 | 0 |
| 5 | MES access | MESaccess | 100 | 0 |
| 6 | MES agregation | MESagregation | 100 | 0 |
| 7 | MES devices | MESaccess | 100 | 0 |
| 8 | MySQL server | MYSQL | 2 | 0 |
| 9 | PORTAL servers | PORTAL | 2 | 0 |
| 10 | RADIUS servers | RADIUS | 2 | 1 |
| 11 | SSW servers | SSW | 2 | 0 |
| 12 | WIRELESS devices | WEP-12ac, WEP-12ac-RevB, WEP-12ac-RevC, WEP-2ac, WEP-2ac-Smart, WOP-12ac, WOP-12ac-ER, WOP-12ac-LR, WOP-12ac-LR-RevB, WOP-12ac-LR-RevD, WOP-12ac-RevB, WOP-12ac-RevC, WOP-2ac | 200000 | 9 |
| 13 | WIRELESS devices by external vendors | GenericAp | 1000000 | 0 |
| **Total** | | **29** | **1201411** | **12** |

# Admin Panel licenses

## Purpose

The number of users that can be logged in Admin Panel and work with its WEB interface simultaneously is limited by licenses.

Administrative accounts (e.g. 'admin') are not included in the total number of logged in users when new accounts are created. However, they are included there when the number of simultaneous website visitors is calculated (when entering Admin Panel).

## Licensing procedure and installation

A license file is not included into `eltex-wifi-cab` package by default. In this mode, a demo license for 5 users can be used to evaluate the system.

Eltex specialists will generate a personal license file and create a e-Token key in the acquisition of licenses.

e-Token should be connected to a server's USB interface. If a server operates on a virtual machine, the key should be forwarded to a virtual machine.

The license file should be put into the following directory:

```
/etc/eltex-wifi-cab/
```

After that, tomcat service should be restarted.

## Verification

To check if licenses have been applied successfully, select "License" in "Help" tab of GUI EMS. Information on the current license and users number restrictions will be available in the opened window.

# PCRF licenses

## Purpose

Checks the number of PCRF Wi-Fi users' sessions and enables/disables session management scenarios.

## Licensing procedure and installation

A license file is not included into eltex-pcrf package by default. In this mode, a demo license for 1000 BRAS sessions can be used to evaluate how the system performs without scenarios.

Eltex specialists will generate a personal license file in the acquisition of licenses.

The license file should be put into the following directory:

```
/etc/eltex-pcrf/
```

After that, eltex-pcrf service should be restarted.

## Verification

To check if licenses have been applied successfully, open PCRF WEB console http://server_ip:7070/licence in the "License" section. Information on the license installed will be available on the page.


```
{
  "licence" : {
    "scriptsEnabled" : "true",
    "companyId" : "eltex",
    "licenceId" : "[redacted]",
    "author" : "Жиганов С.В.",
    "activeSessions" : "15000",
    "company" : "Элтекс_Текст",
    "expireDate" : "2018-08-18",
    "etokenSerial" : "[redacted]",
    "version" : "2.0",
    "createDate" : "2016-11-21"
  },
  "licence_default" : {
    "scriptsEnabled" : "false",
    "activeSessions" : "1000"
  },
  "licence_check_interval_s" : 3,
  "licence_last_check" : null
}
```


# RADIUS certificates

## Purpose

The certificate confirms reliability of RADIUS server during EAP validation. A client's device should trust the server certificate for Wi-Fi users successfull authorization.

At the first connection to SSID, a user will be offered to accept the certificate (trust it). Information on certificate's validity and subject will be also available.

## Licensing procedure and installation

The certificate can be issued by various certification centers.

Eltex certificate signed by Comodo is included into SoftWLC package. It is valid for one year. SoftWLC update package will be released prior to the expiry.

## Verification

To check certificate's validity, run the command:

```
     openssl x509 -text -noout -in /etc/freeradius-domain/certs/
radius_eltex_nsk_ru.crt | grep -A4 "Issuer:"
```

The result will include information on the issuer, validity and subject:

```
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited,
CN=COMODO RSA Domain Validation Secure Server CA

        Validity

            Not Before: Sep 26 00:00:00 2016 GMT

            Not After : Dec  1 23:59:59 2017 GMT

        Subject: OU=Domain Control Validated, OU=EssentialSSL,
CN=radius.eltex.nsk.ru
```

# GUI EMS certificates

## Purpose

The certificate confirms reliability of the software developed in Java and executed on a user's computer. Starting and running the program in the absence of the certificate may cause security bugs.

## Licensing procedure and installation

The certificate is used during eltex-ems package compilation, no extra installation needed.

## Verification

Not required.