CALLUP Roam Home SMS

Product Description

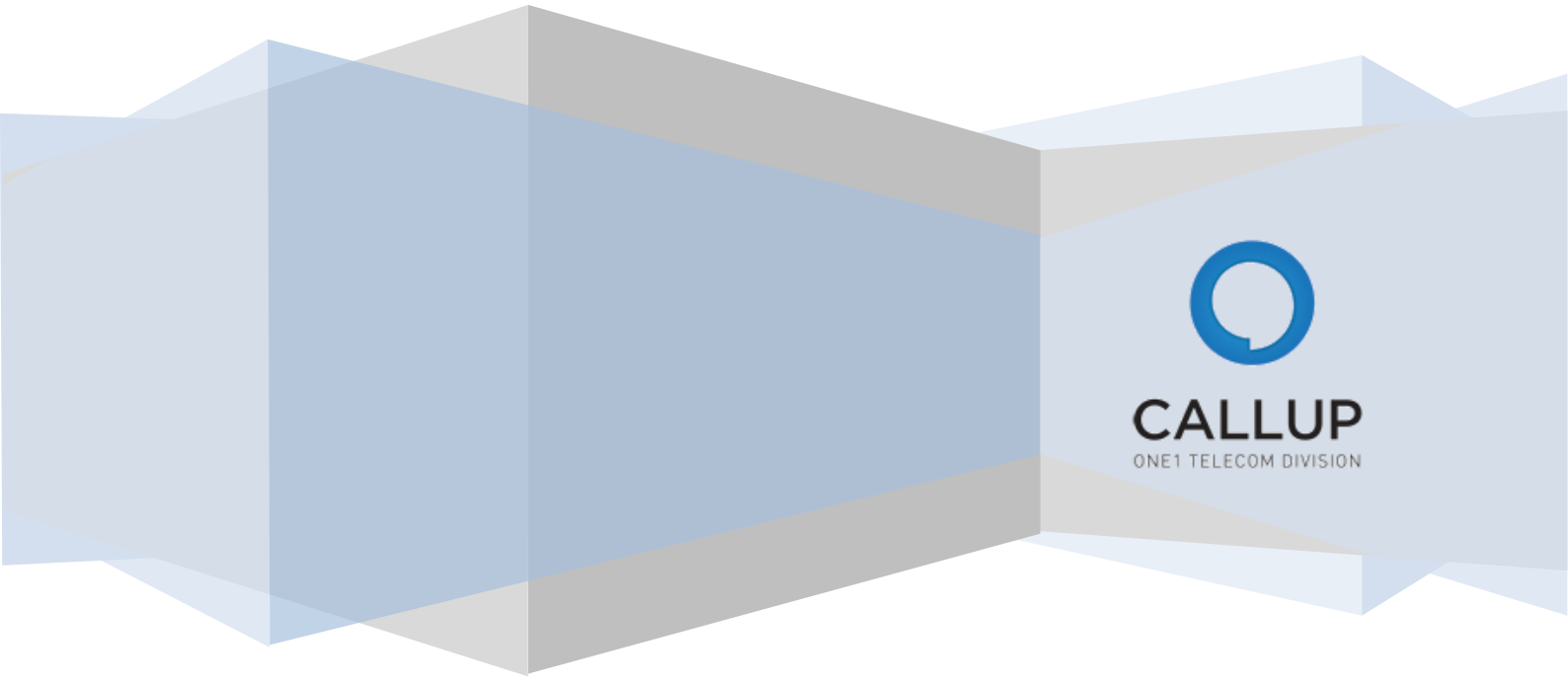


Table of Contents

CALLUP Roam Home SMS Product Description

1. Overview

1.1. About CALLUP

CALLUP net is a subsidiary of the One1 Group, headquartered in Israel and traded in the Tel-Aviv Stock Exchange TASE (Symbol: ONE). Founded in 1999 and has been a leading reliable provider of Value Added Services and Mobile Device Management Solutions for the telecom industry for over a decade.

1.2. About CanVAS

The CALLUP CanVAS platform offers a complete messaging and voice solution that inter-connects Mobile, Land Line and Internet subscribers composing any Value Added Service an operator requires. This document describes the CALLUP Roam Home SMS component of this platform.

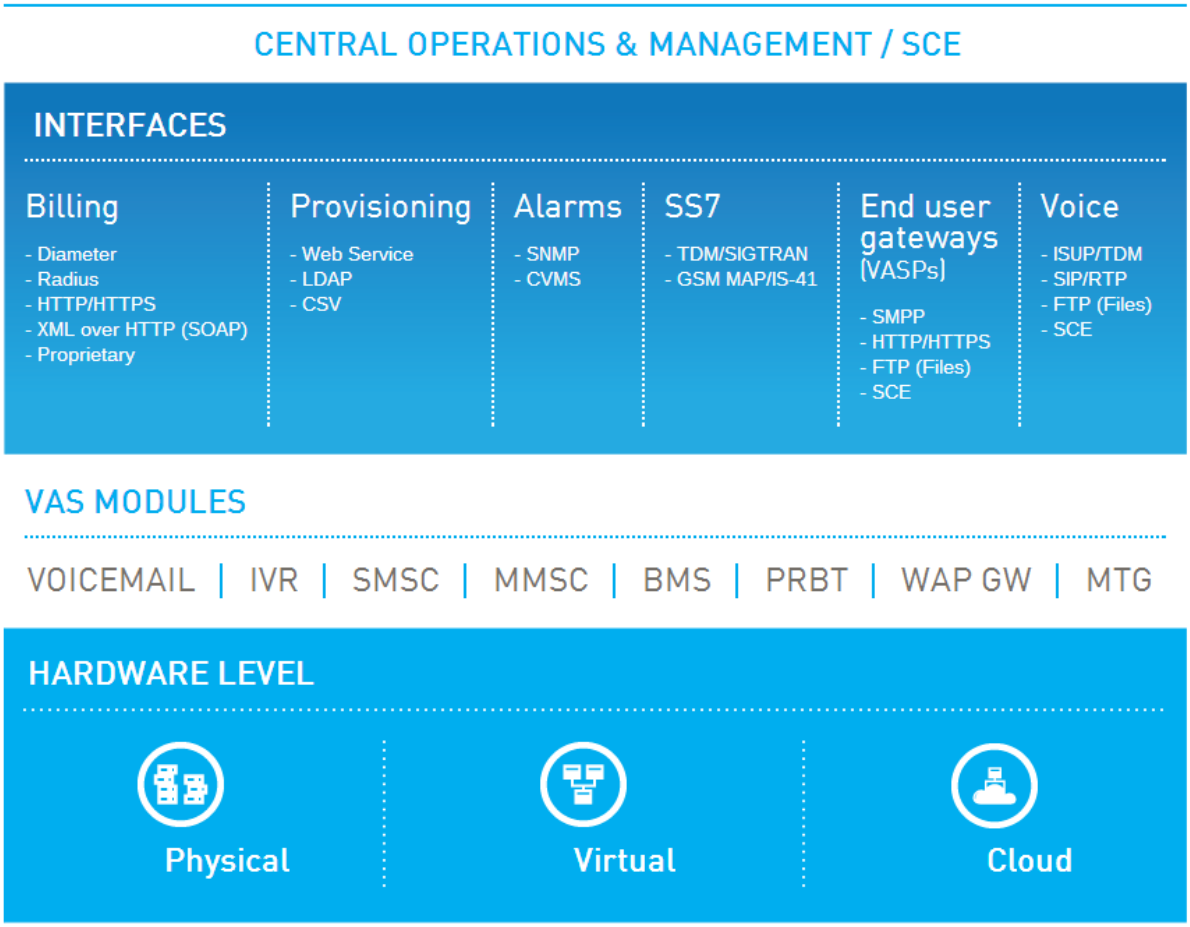


Figure 1 – CanVAS Platform

1.3. About Roam Home SMS

Roam Home SMS is an innovative solution, that helps mobile operators cut down on SMS costs. When a subscriber is roaming, either national roaming or international roaming, and sends an SMS - the operator needs to pay the hosting network, according to the agreements between the operators. With Roam Home SMS – operators can save on these interconnection costs.
The solution seamlessly takes the SMS down from the regular circuit switch path, and sends it via the data network path. The data network can be a cellular data network available, WiFi, or any other internet connection.
The solution does not require the end user to do anything different from his usual SMS sending use case. The end user uses the same SMS interface he normally does, and maintains the same user experience. The re-routing is done behind the scenes.

The solution is based on client-server architecture. The client is located both on the device and on the SIM card, transparent to the user. The server is a gateway to the operator's SMSC which receives the MO messages over IP from the clients and generates CDR's accordingly.

1.4. Roam Home SMS High Level Features

Feature	Description
SMS Capture	Seamlessly capture an outgoing SMS from being sent over the circuit switch network, and divert it to the data network. User maintains regular SMS user experience.
Delivery Reports	Delivery reports, if requested, are delivered back to the sender, with the correct delivery status.
Active Networks Control	Control which networks will be active: • International Roaming • National Roaming • Home network • Specific networks • Any combination of the above
SSL and Anti-spoof Security	Server mechanisms ensure the validity and authenticity of the sender, which allows accepting messages from Wi-Fi/Internet over HTTPS.
Data Network Control	Control what type of data networks will be active: • Cellular or WiFi • Cellular Only • WiFi Only
CDR Generation	Detailed CDRs on every incoming and outgoing message which passes though the server.
Statistics and Reports	Detailed usage reports, usage statistics, available from CVMS - the web management console.
Detailed Logger	Detailed logger which enables troubleshooting and problem investigation easily.

OTA Client Configuration	Server can control the configuration of the clients remotely. Multiple configuration profiles are supported.
SNMP Alarms	Alarms on various hardware and software events, sent to NOC over SNMP
Black/White lists	Block: • Specific devices (IMEIs) • IMEI ranges • Specific subscribers (IMSI/MSISDN) • IMSI/MSISDN ranges • Specific device model, OS version, device manufacturer • MCC/MNC ranges

2. Solution Architecture

2.1. Diagram

The following is a block diagram that describes in high level the various elements of the solution:

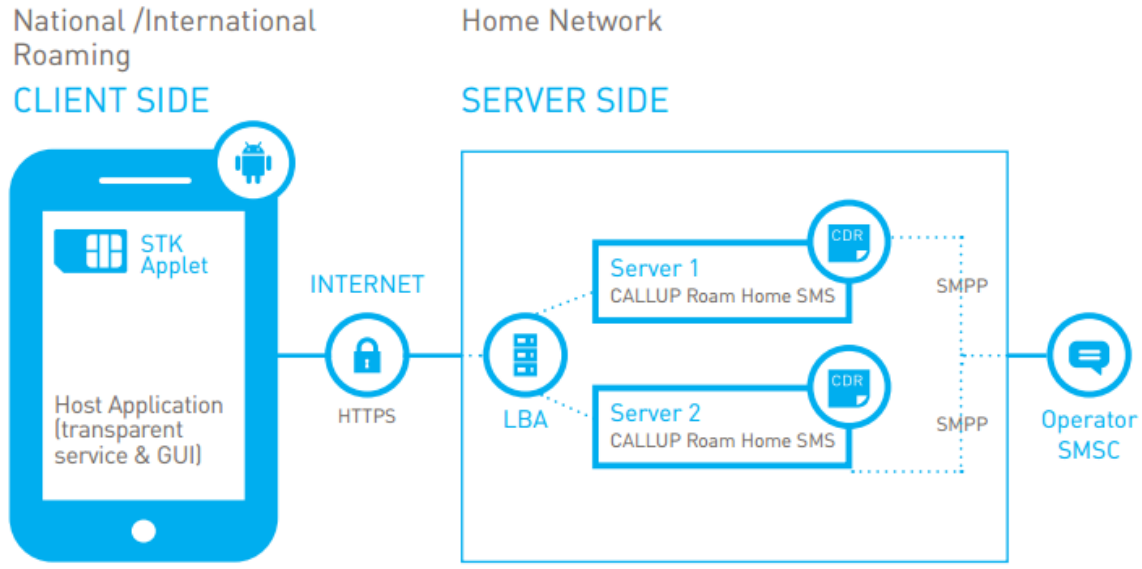


Figure 2 - High Level Block Diagram

- The client is composed of two elements, an application on the phone OS, and an application on the SIM card (STK applet).
- The server is a redundant and scalable solution, composed of a load balancer and N servers (2 in the diagram), that accept the SMS requests over HTTPS from the client application, terminate it in the network using the operator's SMSC (using SMPP), and deliver the status back to the client.

2.2. Usage Call Flow

The following diagram displays the flow of SMS capture and redirection:

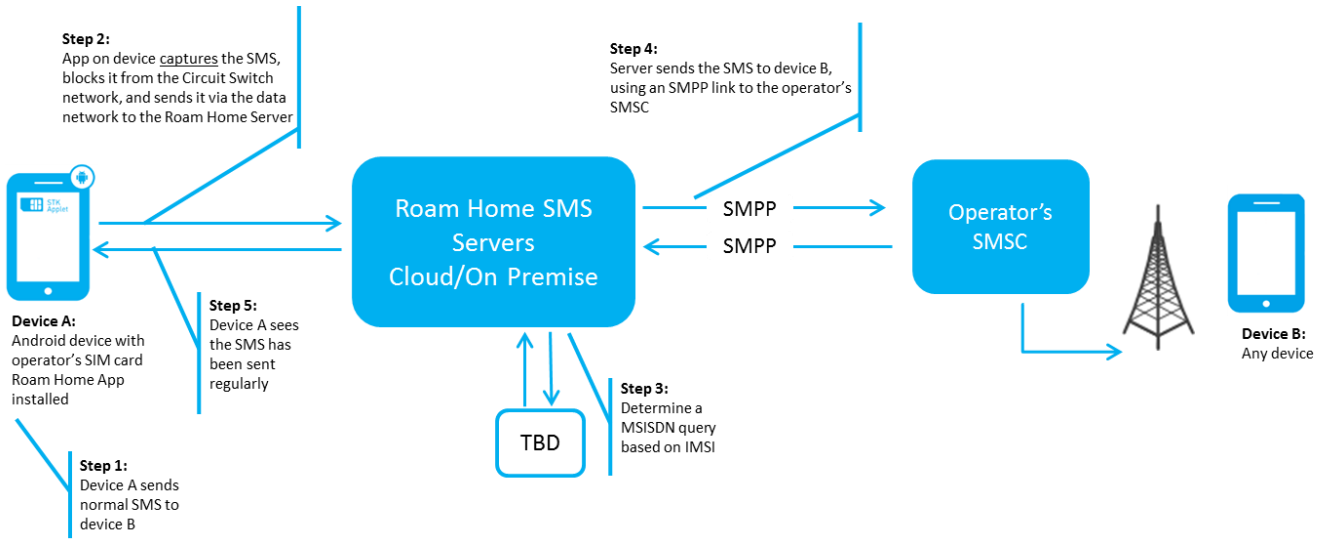


Figure 3 - Simplified Call Flow

2.3. Installation Options

2.3.1. Physical

The system can be provided as a physical installation at the customer's premises. CALLUP can provide the hardware itself, or a list of required hardware that the customer can purchase.
CALLUP uses standard servers primarily from HP. For load balancer CALLUP usually provides F5.
A typical installation consists of:

- 2 HP servers
- 2 Load balancers
- Rack mount, IP switches and other peripherals are optional. CALLUP can provide if required.

2.3.2. Virtual

The system can be deployed on an already existing virtualization farm that the operator maintains. CALLUP can provide its solution as a preconfigured virtual machine, ready to be installed on the existing infrastructure. Supported hypervisors include VMWare and Hyper-V.

2.3.3. Cloud (Private Cloud)

CALLUP can provide the computing and networking services using cloud computing companies, such as Amazon Web Services. A VPN is created between the private cloud network and the customer's network. This essentially creates servers which are virtually in the operator's network, even though physically they are located at a datacentre in the region.
This method eliminates the hassle of working with physical hardware, taking care of hardware failures, support contracts and SLAs, power consumption etc.
Amongst other benefits of a cloud solution:

- Managed service
- Solution resources aren't dictated by peaks
- Gradual growth

3. Solution Overview

The solution is composed of the following modules:

1. Client application
    a. Application running on the handset OS
    b. Application running on the SIM card (STK applet)
2. Server application

The following sub chapters will provide more information on each module.

3.1. Client application details

The client application needs to be installed on the handset for this solution to work. Getting it installed on the client is a challenge. Depending on the business scenario, there might be several paths for this:

- As a hidden feature of another application. For example, the operator's portal application, billing information application, voicemail/VAS settings application etc. This way, the roam home is installed behind the scene, and the subscriber is not aware of the SMS routing.
- As a dedicated application - assuming the marketing provides some incentive for the subscriber, you can provide benefits for subscribers who download and install it.

The second part of the client application is the STK applet. Without the applet, the client application captures ~90% of the SMSs. But with the STK applet, 100% of the SMSs are captures and routed via the data network when one is available. CALLUP releases the STK as a binary file. The current applet size is ~4K.
The operator may use its OTA systems to deploy the applet, and can also include it in the SIM profile such that new SIM cards come built in with it.
If required, as a provider of SIM OTA systems, CALLUP can offer the applet deployment service as well.

Currently the client application is supported on Android and Blackberry devices only.

3.2. Server application details

The server side part of the solution is a Telco grade high availability and high performance solution which is built to serve hundreds of transactions per second.

Main supported features on the server side:

- SNMP for monitoring, management and alerts.
- CVMS management through web GUI
- Full logging for tracing the system activity
- CDRs and SDRs creation
- Secured (see security part below)
- Support dynamic runtime configuration change with zero downtime
- IMSI caching

3.3. Security

A major factor that is important to validate is making sure that the sender is authentic. Since the server is running and available to all through the internet, an extra caution should take place.
The client-server communications are based on TLS or HTTPS, the client validates the server SSL certificates and a special hashing algorithm based on the IMSI of the sender and other parameters are validated on the server to prevent spoofing and hackers tampering.
The server also uses internal spoofing and protection algorithms to identify miss-use or any other abnormal activities. Alerts on hacking attempts and defense activity mechanisms are implemented to prevent these on runtime.

4. Interfaces

4.1. Billing

Node Name	Protocol	Description	Physical Connectivity
Billing/OSS	CDR over FTP/ Diameter/Any	CDRs /online charging for prepaid.	Ethernet

For example, these are examples of the fields the CDR contains:

- Sender MSISDN
- Sender IMSI
- Sender Location Information
- Destination Number
- Date and time
- Client application version
- Delivery report requested
- STK installed / version
- Sender's IMEI
- SMS content length

4.2. Network

The Roam Home SMS interacts with the following network elements:

Node Name	Protocol	Description	Physical Connectivity
IP Network	IP	Connects to the various networks for IT, billing, SS7, Customer Care, NOC etc.	Ethernet
*STP	SCTP/M3UA	If SRI_4_LCS used, GSM MAP traffic is carried from/towards HLR via the STP.	Ethernet
SMSC	SMPP v3.4	For the actual submission of MT messages, and accepting of delivery reports.	Ethernet

- Note – the STP and SRI4LCS are required to translate the IMSI sent by the clients to their associated MSISDN in the network. Since the clients are not aware of their own MSISDN number they can only send IMSI to the server. The server then, needs to translate IMSI to MSISDN in order to deliver the SMPP message to B party.

  SRI4LCS is optional. If there are any other APIs in the network such as LDAP query or HTTP or any other means to translate IMSI to MSISDN, they can be used instead.

4.3. Provisioning

No provisioning is required for the service. Clients with the application installed will divert the traffic towards the servers, and the servers will handle their requests.

5. Scalability

The Roam Home SMS platform is fully scalable, which means it can be scaled to any number of transaction per second required. If the solution is deployed using the physical installation approach, on the customer's premises, a load balancer machine is required. The application servers run in active-active mode, and are planned with N+1 redundancy scheme (see redundancy chapter).

Generally speaking, an 8 CPU cores machine with 32 GB of RAM can handle up to 250 SMS per second*. This figure should be used as a rule of thumb for the calculation on the hardware required, when designing the hardware for the solution.

** This number represents a typical installation and may vary for specific installations*

6. Redundancy

Roam Home SMS is designed to be robust, with redundancy in every module with no single point of failure, both hardware and software wise.

The typical physical installation includes 2 load balancers and 2 servers. The 2 servers work together in active-active manner. The solution is planned with N+1 redundancy scheme. This means, that if N servers are required for capacity X, then N + 1 servers will be used. For example, let's say you need a 500 TPS system. Two servers can handle this load, but the system will be deployed with 3 servers - to allow the backup in case one server fails.

7. Standard Compliancy

The system is compliant* with the following standards:

- Hypertext Transfer Protocol -- HTTP/1.1
- Hypertext Transfer Protocol Secure (HTTPS)
- SOAP Web Services
- TLS / SSL (RFC5246, RFC 2246)
- SMPP v3.4
- GSM MAP Rev. 1/2/3

** The relevant parts of the standard which are required for the operation of the server*

8. O&M

8.1. Administration

The Roam Home SMS service is administered via a rich web based GUI tool called CVMS. CVMS enables for example service start and stop, status view, host machine information, log file view, configuration parameter changes, configuration file editing and much more.

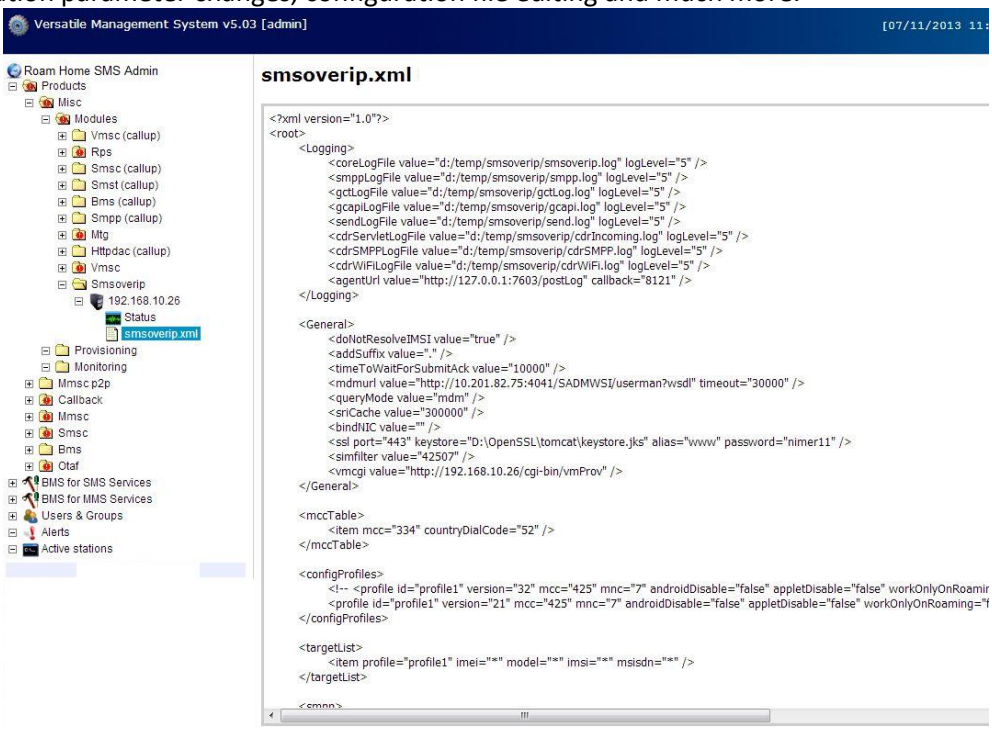
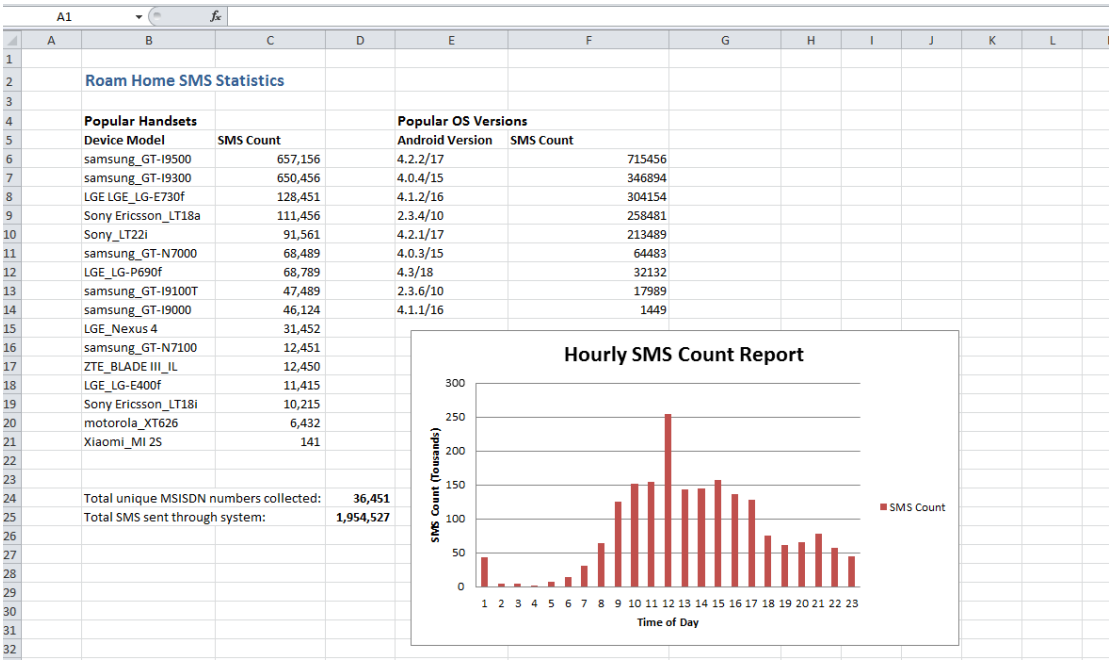


Figure 4 - Editing Configuration File from CVMS

The access to the service's reports and statistics files and interfaces are also done from CVMS.



Roam Home SMS Statistics

Popular Handsets		Popular OS Versions	
Device Model	SMS Count	Android Version	SMS Count
samsung_GT-I9500	657,156	4.2.2/17	715456
samsung_GT-I9300	650,456	4.0.4/15	346894
LGE LGE_LG-E730f	128,451	4.1.2/16	304154
Sony Ericsson_LT18a	111,456	2.3.4/10	258481
Sony_LT22i	91,561	4.2.1/17	213489
samsung_GT-N7000	68,489	4.0.3/15	64483
LGE_LG-P690f	68,789	4.3/18	32132
samsung_GT-I9100T	47,489	2.3.6/10	17989
samsung_GT-I9000	46,124	4.1.1/16	1449
LGE_Nexus 4	31,452		
samsung_GT-N7100	12,451		
ZTE_BLADE III_IL	12,450		
LGE_LG-E400f	11,415		
Sony Ericsson_LT18i	10,215		
motorola_XT626	6,432		
Xiaomi_MI 2S	141		

Total unique MSISDN numbers collected:	36,451
Total SMS sent through system:	1,954,527

Figure 5 - Example Report

8.2. Monitoring

CVMS is also utilized for system monitoring. All alerts, with all severities, are collected by CVMS and can be viewed, filtered, and in general provide a quick understanding of the system status. The nodes with the various modules are highlighted with different colours, until the alarm is cleared by the operator.

9. Licensing options

Feature	Standard	Advanced
SMS Capture	**x**	
Delivery Reports	**x**	
Active Networks Control	**x**	
SSL and Anti-spoof Security	**x**	
Data Network Control	**x**	
CDR Generation	**x**	
Statistics and Reports	**x**	
Detailed Logger	**x**	
OTA Client Configuration		**x**
Black/White lists		**x**
SNMP Alarms	**x**	