Oracle Communications Mobile Security Gateway-Accuris Networks AccuROAM Integration in Apple Wi-Fi Calling Application

Technical Application Note

Technical Application Note

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This document is intended for use by Oracle Sales Consultants, Engineers, third party Systems Integrators, and end users of the Oracle Communications Session delivery network product portfolio namely Mobile Security Gateway, Session Border Controller, Core Session Manager. It assumes that the reader is familiar with basic operations of the Oracle Communications 4600/6100/6300 platforms.

Document Overview

This technical application note documents the Oracle Mobile Security Gateway (MSG) and AccuROAM AAA server Integration and interoperability testing in Apple Wi-Fi calling environment. It should be noted that while this application note focuses on the optimal configuration between Oracle Mobile security gateway and the Accuris AccuROAM server, production environments in different customer networks will have additional configuration parameters that are specific to other applications.

Introduction

Wi-Fi Calling

Wi-Fi calling or Voice over Wi-Fi (VoWifi) is the ability to send and receive phone calls and SMS/MMS messages using the Wi-Fi home, office or public hotspot such as coffee shop, airport, shopping mall, etc. The 3GPP Interworking-Wireless LAN (I-WLAN) architecture enables amongst others SIP-based traffic, such as VoLTE, to be routed via unlicensed spectrum, i.e. home or venue Wi-Fi access networks, and to be integrated into the packet core of an Operator. Using I-WLAN, operators and SPs can deliver SIP-based services (such as VoLTE and UC) over unlicensed spectrum with seamless session hand-over between the licensed (LTE) and unlicensed (Wi-Fi) radio access networks. Because Wi-Fi access networks can be untrusted and/or unmanaged, to provide integrity and confidentiality, the I-WLAN standard defines the use of IPSec from the device to the packet core. Alternatively, a downloadable mobile client for VoWifi can utilize SIP/TLS and SRTP to provide integrity and confidentiality. This document focuses on integration between Oracle Communications Mobile Security Gateway and Accuris AccuROAM AAA server with Apple Wi-Fi calling.

Oracle Communications – Accuris Networks Partnership

Oracle Communications Mobile Security Gateway (MSG) is an Evolved Packed Data Gateway (ePDG) in the 3GPP I-WLAN Architecture supporting Wi-Fi Calling. It integrates with 3GPP based AAA server like AccuROAM to provide authentication to devices and IPsec tunnel management using Eextensible Authentication Protocol (EAP-SIM/AKA).

Accuris Networks is a Global Provider of operator networking solutions that deliver intelligent connectivity and dynamic control of the subscriber experience in multi-network environments. Accuris offers specific solutions for internetworking, IMS readiness, Wi-Fi calling and network roaming. The Oracle-Accuris combined solution delivers on all the benefits of Wi-Fi calling–improved customer experience, coverage and reduced macro network costs–with security, manageability and reliability.

Oracle Communications Mobile Security Gateway

Oracle Communications Mobile Security Gateway (hereafter MSG) is a high performance tunneling gateway for heterogeneous networks, enabling fixed mobile convergence and offload macro Radio Access network traffic. It secures the core networks of service providers from untrusted internet access to local femtocells, evolved Home Node Bs (LTE femtocells) and Wi-fi devices. The Mobile Security gateway is supported on the Acme Packet 4600, 6100 and 6300 platforms. It leverages the industry leading Acme Packet OS software platform to offer security gateway capabilities – large scale IPsec tunnel termination from femtocells and Wi-Fi devices into mobile operator core.

The MSG typically deployed in operator’s Core network and is based on industry standards and fulfills the following functional elements defined by Third Generation Partnership Project (3GPP) and

Third Generation Partnership Project Two (3GPP2):

- Interworking-Wireless Local Area Network (I-WLAN) Tunnel Terminating Gateway (TTG)
- Home NodeB (HNB) Security Gateway
- Femtocell Security Gateway
- Evolved Packet Data Gateway (ePDG)

Application Overview

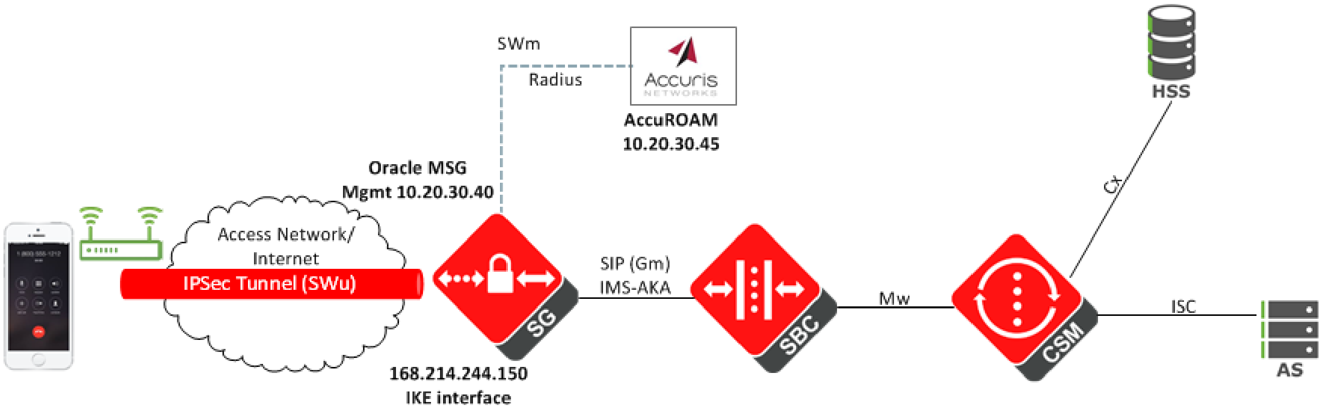
Mobile security gateway provides secure integration from Wi-Fi RAN to Mobile Core. The Wi-Fi network is treated as a separate RAN, the ePDG establishes a secure tunnel over the internet to the specific device so that this “untrusted” traffic can be incorporated into the mobile core.

Oracle-Accuris Wi-Fi calling solution consists of the Accuris eAAA, Oracle MSG and Oracle IMS Core (Oracle SBC/P-CSCF, Oracle CSM) with the following high level capabilities:

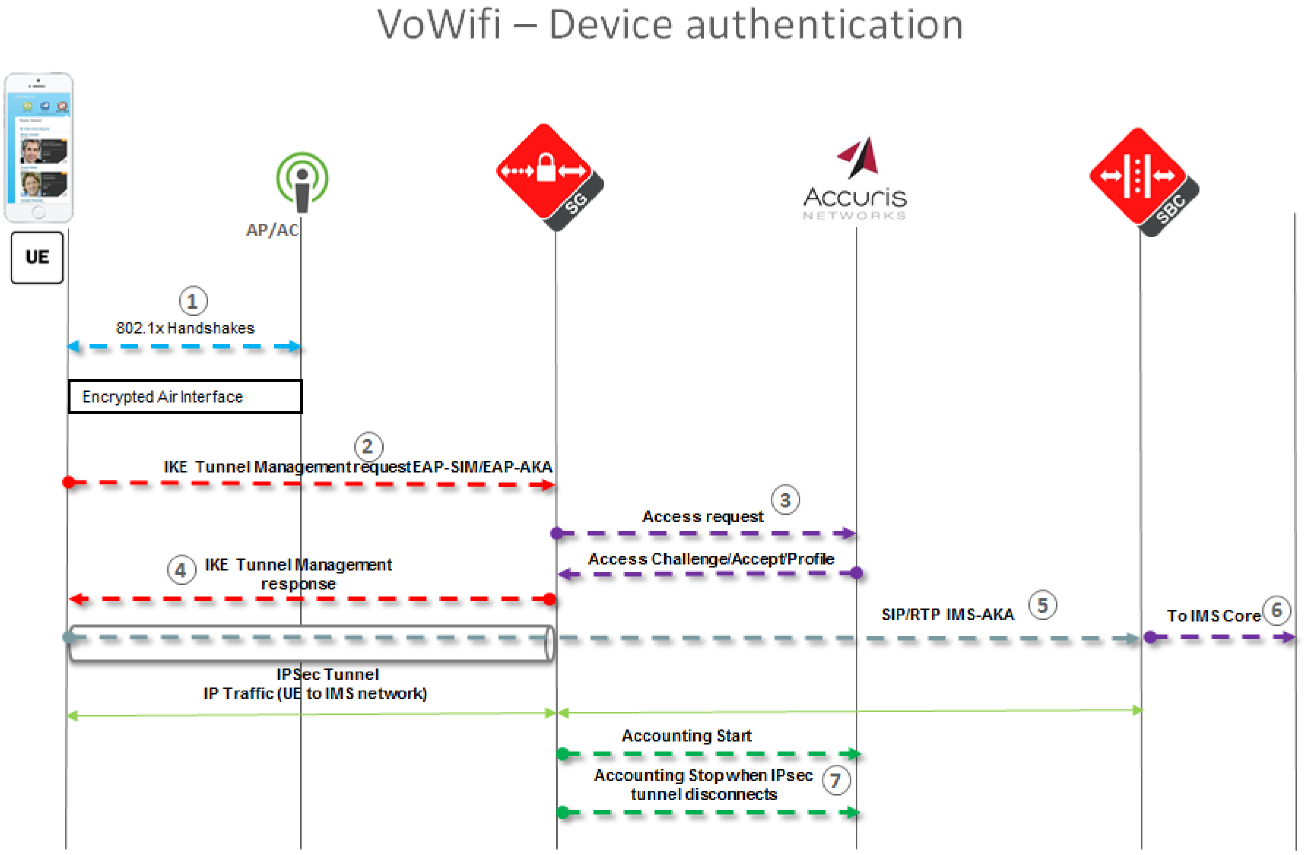
- eAAA: Enhanced AAA functionalities present in the AAA solution
- EAP authentication (EAP-SIM/AKA)
- SWm (RADIUS) interface with Oracle MSG
- SIP IMS-AKA over Gm interface from UE to Oracle SBC/P-CSCF via Oracle MSG
- SWn interface between UE and ePDG

This integration used iPhone 6 devices installed with iOS9 operating system. The devices establishes IPsec tunnel to the Oracle MSG (ePDG). Each device establishes its own IPsec tunnel and used EAP-SIM authentication to authenticate with the AccuROAM AAA via Oracle MSG. Alternatively, service providers may choose to use EAP-AKA based authentication.

Oracle VoWiFi Architecture with Accuris



Device Authentication Overview


VoWifi – Device authentication
UE
AP/AC
SG
Accuris NETWORKS
SBC
1
802.1x Handshakes
Encrypted Air Interface
2
IKE Tunnel Management request EAP-SIM/EAP-AKA
3
Access request
Access Challenge/Accept/Profile
4
IKE Tunnel Management response
SIP/RTP IMS-AKA
5
To IMS Core
6
IPSec Tunnel
IP Traffic (UE to IMS network)
Accounting Start
Accounting Stop when IPsec tunnel disconnects
7

VoWiFi

Subscriber using their mobile device (iPhone 6), connects to Wi-Fi, registers to the VoWifi network and is able to place calls over Wi-Fi using native dialer on the iPhone.

Below is sequence of events when device is powered on to connect to Oracle MSG attach in Wi-Fi network (for VoWifi based registration/call)

1) UE powers on in Wi-Fi access or moves into Wi-Fi access area and performs authentication procedure and selects ePDG (UE may select ePDG via static assignment or dynamically or acquired during LTE attach procedure)
2) UE initiates IPsec tunnel establishment procedure via IKEv2 to ePDG (multiple messages exchanged)
3) The ePDG sends EAP request via RADIUS to AAA server over SWm interface (Access-Request message). AAA server retrieves user profile and sends Access-Challenge/Access-Accept)
4) ePDG completes EAP authentication (gets the challenge from UE and forwards to AAA), responds to UE (IKE tunnel management response)
5) Once the UE is connected over IPsec tunnel to ePDG, it initiates IMS-AKA based registration for authenticating the Gm interface with the IMS Core (P-CSCF which is Oracle SBC) according to IR.92/VoLTE
6) Oracle IMS core (P-CSCF/SBC plus CSM will interact with HSS, download authentication data with digest-akav1-md5 and reg/401/200 OK exchange will take place to register the UE to IMS Core. UE can then initiate VoWifi calls
7) Oracle ePDG can send IKEv2 and IPsec accounting information to AccuROAM server

Lab Configuration and Software/Hardware Tools

The test environment consisted of the following components:

- Oracle Communications Mobile security gateway
- AccuROAM AAA server
- Iphone 6 and 6s plus devices

The following tables provide the software hardware versions used for the elements:

Oracle Communications Mobile Security Gateway System Specifications

Hardware	Acme Packet 4600 platform with 2 x 10 GbE and 4 x 1 GbE NIU
Software Release	nnMCZ400p1.64.bz
Software modules enabled	Security gateway, IKE tunnels (200000 tunnels)

AccuROAM AAA Server specifications

Application	Virtualized
Software Release	8.2.35
Software Modules/Interfaces	SWm (for EAP-SIM authentication), Rekkit for simulating HSS authentication

Apple iPhone Device specifications

Hardware	iPhone 6 and 6s Plus
Software Release	9.1

Configuration of Oracle MSG

In this section we describe the major steps for configuring the Oracle Mobile Security Gateway to connect to AccuROAM server.

In Scope

This section focuses on configuration highlights in MSG to establish connection with AccuROAM server. For detailed concepts and configuration on the MSG, please contact your Oracle representative.

Out of Scope

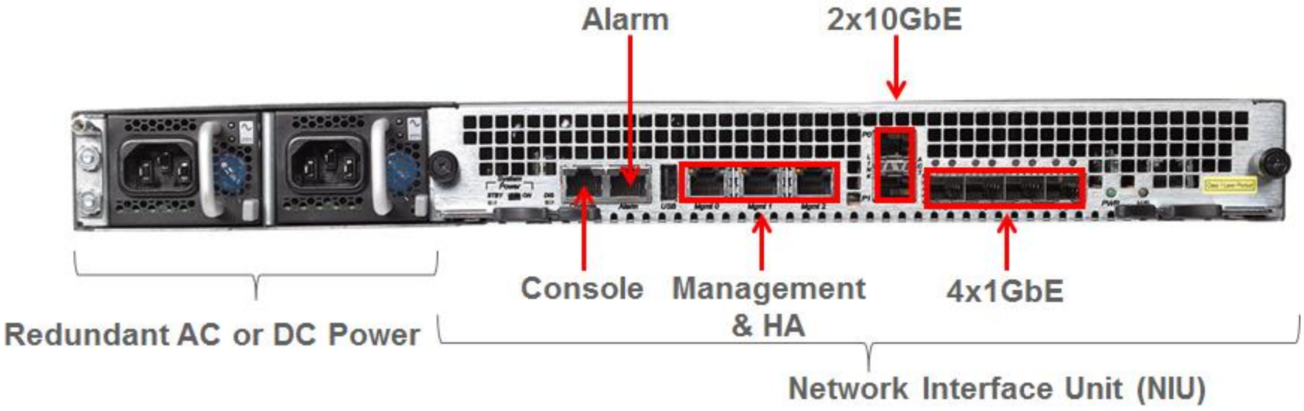
- IMS core configuration and Network management configuration of the MSG

What you will need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle MSG
- IP address to be assigned to management interface (Wancom0) of the MSG - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the MSG is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support configurations with management and media/service interfaces on the same subnet.
- IP address on management subnet of AccuROAM server
- IP addresses to be used for the MSG IKE interface (Access side) and Core side (towards Oracle SBC/P-CSCF)
- IP address of the next hop gateway in the IMS core network

Configuring the MSG

Once the Oracle MSG is racked and the power cable connected, you are ready to set up physical network connectivity.



As seen in the above picture, the 4600 platform has a field replaceable 2 x 10 Gb/sec and 4 x 1 Gb/sec NIU. The NIU supports Enhanced Small Form factor pluggable (SFP+) for the two 10 Gb/sec Ethernet fiber ports and Small form factor pluggable (SFP) for the four 1 GbE ports. Plug the slot 0 port 4 (s0p4, bottom of the two 10GbE interfaces) interface into your outside (Internet facing) network and the slot 0 port 5 (s0p5) interface into your inside (service provider core – IMS network facing) network. Once connected, you are ready to power on and perform the following steps.

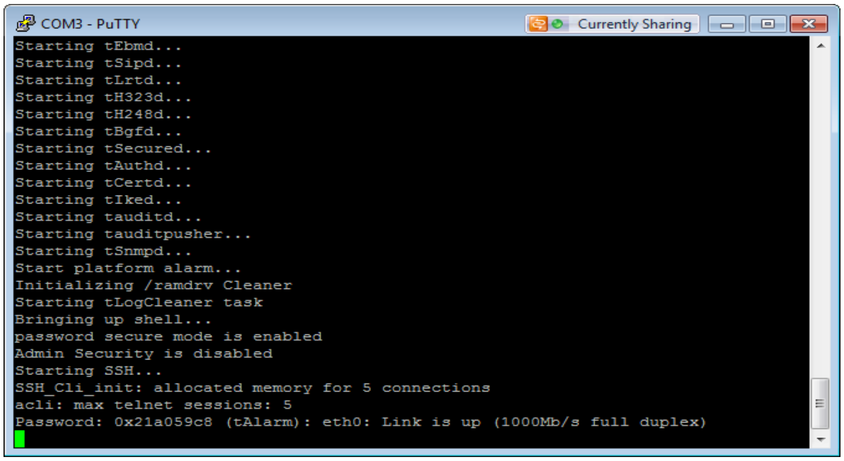
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as VoWifi-MSG are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the MSG

Confirm the MSG is powered off and connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the MSG and the other end to console adapter that ships with the MSG, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as PuTTY. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the MSG and confirm that you see the following output from the bootup sequence.



```
Starting tEbmd...
Starting tSipd...
Starting tLrtd...
Starting tH323d...
Starting tH248d...
Starting tBgfd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Start platform alarm...
Initializing /ramdrv Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH_Cli_init: allocated memory for 5 connections
acli: max telnet sessions: 5
Password: 0x21a059c8 (tAlarm): eth0: Link is up (1000Mb/s full duplex)
```

Enter the following commands to login to the MSG and move to the configuration mode. Note that the default MSG password is "**acme**" and the default super user password is "**packet**".

```
Password: acme
VoWifi-MSG> enable
Password: packet
VoWifi-MSG# configure terminal
VoWifi-MSG(configure)#
```

You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the SBC by going to

VoWifi-MSG#configure terminal --- >bootparams

- Once you type "bootparam" you have to use "carriage return" key to navigate down
- A reboot is required if changes are made to the existing bootparams

```
VoWifi-MSG#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device                : eth0
processor number           : 0
host name                  : acmesystem
file name                  : /boot/nnMCZ400p1.64.bz --- >location where the
software is loaded on the MSG
inet on ethernet (e)       : 10.20.30.40:ffffff80 --- > This is the ip
address of the management interface of the MSG, type the IP address and
mask in hex
inet on backplane (b)      :
host inet (h)              :
gateway inet (g)           : 10.20.30.40.1 --- > gateway address here
user (u)                   : vxftp
ftp password (pw) (blank = use rsh)      : vxftp
flags (f)                  :
target name (tn)           : VoWifi-MSG
startup script (s)         :
other (o)                  :
```

The following section walks you through configuring the Oracle Communications MSG configuration required to work with AccuROAM AAA server. The MSG is largely in pass through mode for EAP based authentication transferring the IMSI credentials to the AccuROAM server and using certificate to authenticate itself with the device.

High Availability

The wancom1 and wancom 2 port which is on the rear panel of the 4600 system is used for the purpose of High Availability. Please refer to the Oracle Session Border Controller SCZ 7.2.0 ACLI Configuration guide for more detailed update on High availability configuration. (http://docs.oracle.com/cd/E55601_01/doc/sbc_scz720_acliconfiguration.pdf)

The following section entails notable configuration highlights that pertain to EAP based authentication and accounting with AccuROAM AAA server. A full copy of the configuration that was used for this integration is elaborated in the appendix section as well.

Configuration Highlights

The MSG configuration follows in general a security gateway configuration per the concepts outlined in the security gatway essentials guide available at http://docs.oracle.com/cd/E67896_01/doc/sg_mcz400_essentials.pdf

In this section, the authentication, accounting, new configuration containers and their references in MCZ400p1 image along with additional security policy for processing IMS-AKA encrypted traffic between UE and P-CSCF are highlighted.

Authentication and Accounting

To define the AccuROAM server for authentication and accounting, following steps are required:

- Define Authentication element and reference the IP address of the AccuROAM server
- Define auth-params element
- Define account-group element and configure IP address of AccuROAM for accounting
- Define Ike-accounting-param and choose type of accounting records
- Reference accounting-param name and authentication server in security-interface-params
- Reference the security-interface-params in ike-interface

Authentication

We define an authentication element in the security configuration to define the AccuROAM server and configure the secret (password) as show below:

```
authentication
        source-port                             1812
        type                                    radius
        protocol                                pap
        tacacs-authorization                    enabled
        tacacs-accounting                       enabled
        server-assigned-privilege               disabled
        allow-local-authorization               disabled
        login-as-admin                          disabled
        management-strategy                     hunt
        ike-radius-params-name                  tradius
        management-servers                      10.20.30.45
        radius-server
                address                                 10.20.30.45
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  taqua
                realm-id
                retry-limit                             3
                retry-time                              5
                maximum-sessions                        255
                class                                   primary
                dead-time                               10
                authentication-methods                  all
```

Auth-params

Define the authentication server in auth-params under configure terminal --- > security ---- > auth-params

```
auth-params
        name                                    tradius
        protocol                                eap
        strategy                                hunt
        servers                                 10.20.30.45
        authorization-servers
        options
```

Account-group

Configure an account-group for adding accouting server with secret/password under configure terminal --- > account-group

```
account-group
        name                                    AccuRoam
        hostname                                localhost
        acct-protocol                           RADIUS
        acct-src-port                           1813
        acct-strategy                           Hunt
        account-servers
                hostname                                10.20.30.45
                port                                    1813
                state                                   enabled
                min-round-trip                          250
                max-inactivity                          60
                restart-delay                           30
                bundle-vsa                              enabled
                secret                                  ********
                NAS-ID                                  Oracle-SG
                priority                                0
                origin-realm
                domain-name-suffix
                watchdog-ka-timer                       0
                diameter-in-manip
                diameter-out-manip
        options
```

Ike-accounting-param

Configure ike-accounting-param and choose the type of accounting records you want system to send to AAA server. We set the following accounting events:

- Start: To trigger an accounting request start when an IPSec tunnel is established
- Stop: To trigger an accounting request stop on tunnel tear down
- Interim_ipsec_rekey: To trigger an Interim-Update accounting record when IPsec tunnel rekeying occurs
- Interim_ike_rekey: To trigger an Interim-Update accounting record when IKE tunnel SA rekeying occurs

```
ike-accounting-param
        name                                    Accu-accounting
        radius-accounting-events                start
                                                stop
                                                interim_ipsec_rekey
                                                interim_ike_rekey
        diameter-accounting-events
        intermediate-period                     0
```

Reference accounting-param and authentication server in security-interface-params

```
security-interface-params
        identifier                              ike-vowifi
        address-assignment                      local
        authentication-servers                  10.20.30.45
        authorization-servers
        accounting-params-name                  Accu-accounting
        account-group-list                      AccuRoam
        local-address-pool-id-list              addr-pool
        sg-policy-list
        options
```

Reference security-interface-params in the ike-interface

```
ike-interface
        state                                   enabled
        address                                 168.212.244.150
        realm-id                                public
        ike-mode                                responder
        dpd-params-name                         dpd-SG
        v2-ike-life-secs                        82800
        v2-ipsec-life-secs                      600
        v2-rekey                                enabled
        multiple-authentication                 disabled
        multiple-child-sa-mode                  none
        shared-password                         ********
        options
        eap-protocol                            eap-radius-passthru
        sd-authentication-method                certificate
        certificate-profile-id-list             osegw.ellocloud.net
        threshold-crossing-alert-group-name
        cert-status-check                       disabled
        cert-status-profile-list
        access-control-name
        traffic-selectors
        ip-subnets
        authorization                           disabled
        tunnel-orig-name-list
        security-interface-params-name          ike-vowifi
```

Additional Security-policy for processing IMS-AKA traffic

An additional security-policy is needed in the Oracle MSG for processing IMS-AKA encrypted traffic between UE to P-CSCF. This policy is applied on the core network-interface (operator's core protected network) from where subsequent IMS-AKA protected signaling (ESP) traffic will arrive. The priority of this policy should be set lower than all other policies on this network-interface. The trans-sub-protocol-match field must be set to 50 (IP protocol code for ESP)

```
security-policy
        name                           allow-esp
        network-interface              s1p0:0
        priority                       101
        local-ip-addr-match            0.0.0.0
        remote-ip-addr-match           0.0.0.0
        local-port-match               0
        local-port-match-max           65535
        remote-port-match              0
        remote-port-match-max          65535
        trans-protocol-match           ALL
        trans-sub-protocol-match       50
        trans-sub-protocol-code-match  unknown
        direction                      both
        local-ip-mask                  0.0.0.0
        remote-ip-mask                 0.0.0.0
        action                         allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                  255.255.255.255
                remote-ip-mask                 255.255.255.255
                local-port-mask                0
                remote-port-mask               0
                trans-protocol-mask            0
                valid                          enabled
                vlan-mask                      0x000
```

Configuration in AccuROAM Server

The AccuROAM server was installed in a VMware environment and to simulate HLR interaction a tool called Rekkit was installed. The AccuROAM acts as a VLR receiving IMSI from the device via MSG, sends this sent auth info request to Rekkit which is acting as HLR and expects authentication triplets to authenticate the IMSI. The Oracle MSG uses the SWm interface based on RADIUS protocol over its management interface to send IMSI information received from the device.

In Scope

- Adding Radius cients, secret, auth triplets configuration in AccuROAM

Out of Scope

Installation, network connections/management to Oracle MSG

What you will need

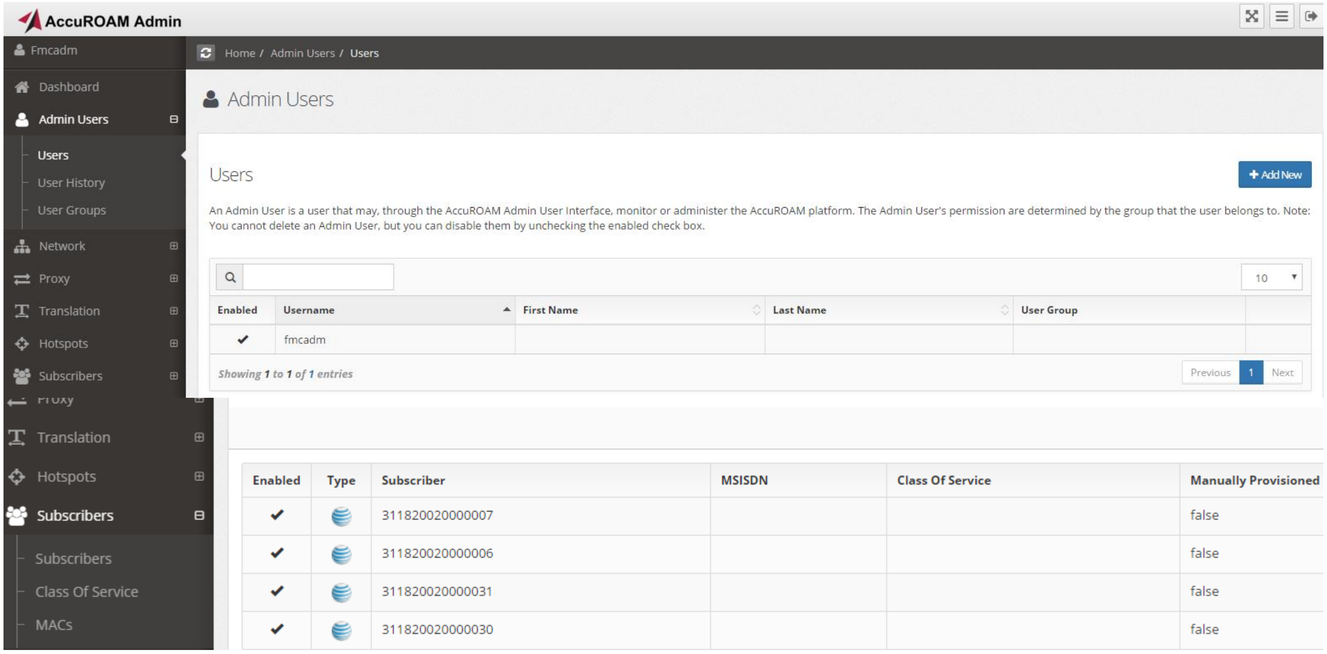
AccuROAM server installed and base SS7 stub with Rekkit tool installed

Configuration in AccuROAM consists of the following steps

- Logging in with user
- Adding/viewing subscribers/IMSI values (auto added when device registers)
- Adding RADIUS client group
- Adding RADIUS client (MSG)
- Add RADIUS server group
- Add RADIUS server (AccuROAM)
- Define Routing
- Configure Accounting route

Logging in

The AccuROAM is available at http://ip-address with username/password as fmcadm/fmcadm



Admin Users

Users

An Admin User is a user that may, through the AccuROAM Admin User Interface, monitor or administer the AccuROAM platform. The Admin User's permission are determined by the group that the user belongs to. Note: You cannot delete an Admin User, but you can disable them by unchecking the enabled check box.

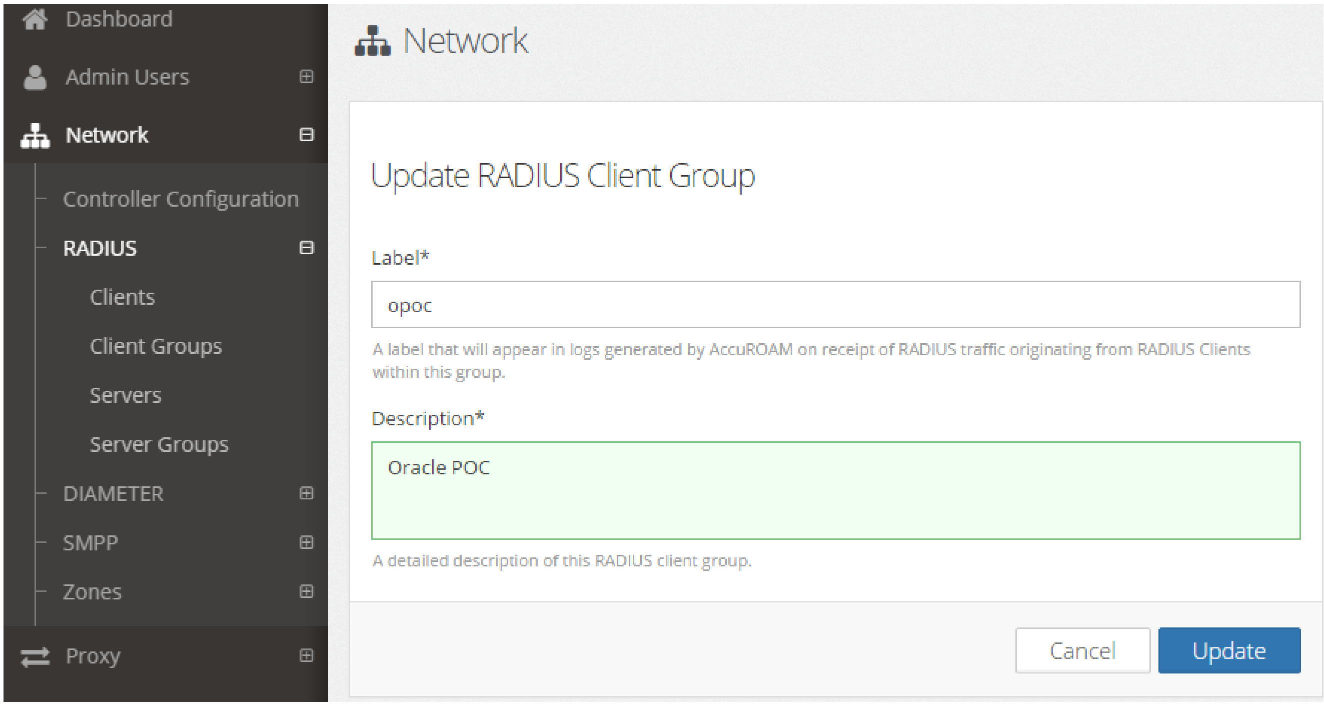
Enabled	Username	First Name	Last Name	User Group
✓	fmcadm			

Showing 1 to 1 of 1 entries

Enabled	Type	Subscriber	MSISDN	Class Of Service	Manually Provisioned
✓	●	311820020000007			false
✓	●	311820020000006			false
✓	●	311820020000031			false
✓	●	311820020000030			false

Add Radius Client Group

Create RADIUS client group under Network ---- > RADIUS --- > Client Group. Click on **Add New.** Create new with the following settings



Update RADIUS Client Group

Label*

opoc

A label that will appear in logs generated by AccuROAM on receipt of RADIUS traffic originating from RADIUS Clients within this group.

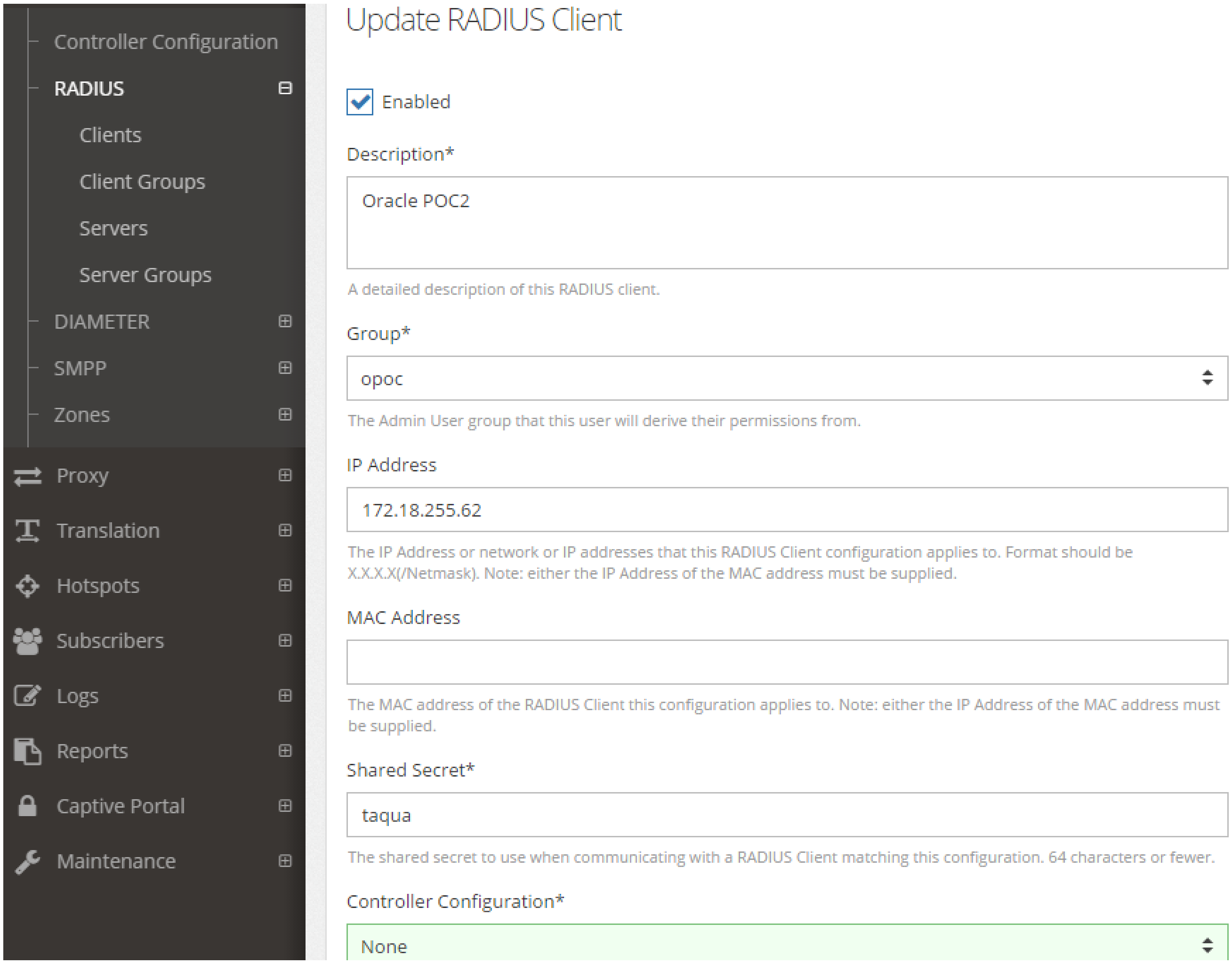
Description*

Oracle POC

A detailed description of this RADIUS client group.

Add Radius Client (Oracle MSG IP address)

To add MSG IP address, cick on Clients under Network ---- > RADIUS. Click on **Add New.** Create new with the following settings



Update RADIUS Client

☑ Enabled

Description*

Oracle POC2

A detailed description of this RADIUS client.

Group*

opoc

The Admin User group that this user will derive their permissions from.

IP Address

172.18.255.62

The IP Address or network or IP addresses that this RADIUS Client configuration applies to. Format should be X.X.X.X(/Netmask). Note: either the IP Address of the MAC address must be supplied.

MAC Address

The MAC address of the RADIUS Client this configuration applies to. Note: either the IP Address of the MAC address must be supplied.

Shared Secret*

taqua

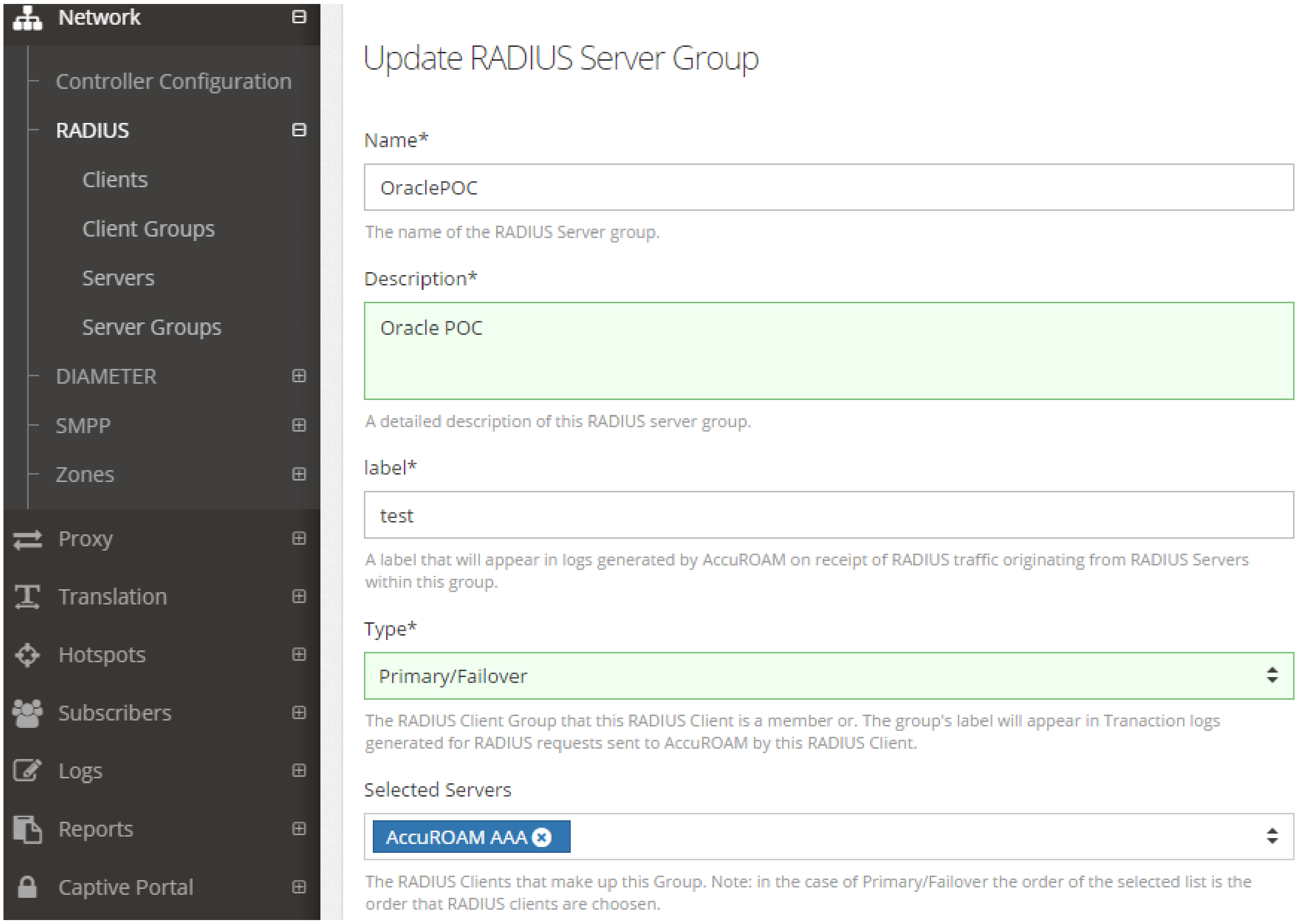
The shared secret to use when communicating with a RADIUS Client matching this configuration. 64 characters or fewer.

Controller Configuration*

None

Add RADIUS Server group

Create RADIUS server group for AccuROAM under Network ---- > RADIUS ---- > Server Groups



Update RADIUS Server Group

Name*

OraclePOC

The name of the RADIUS Server group.

Description*

Oracle POC

A detailed description of this RADIUS server group.

label*

test

A label that will appear in logs generated by AccuROAM on receipt of RADIUS traffic originating from RADIUS Servers within this group.

Type*

Primary/Failover

The RADIUS Client Group that this RADIUS Client is a member or. The group's label will appear in Tranaction logs generated for RADIUS requests sent to AccuROAM by this RADIUS Client.

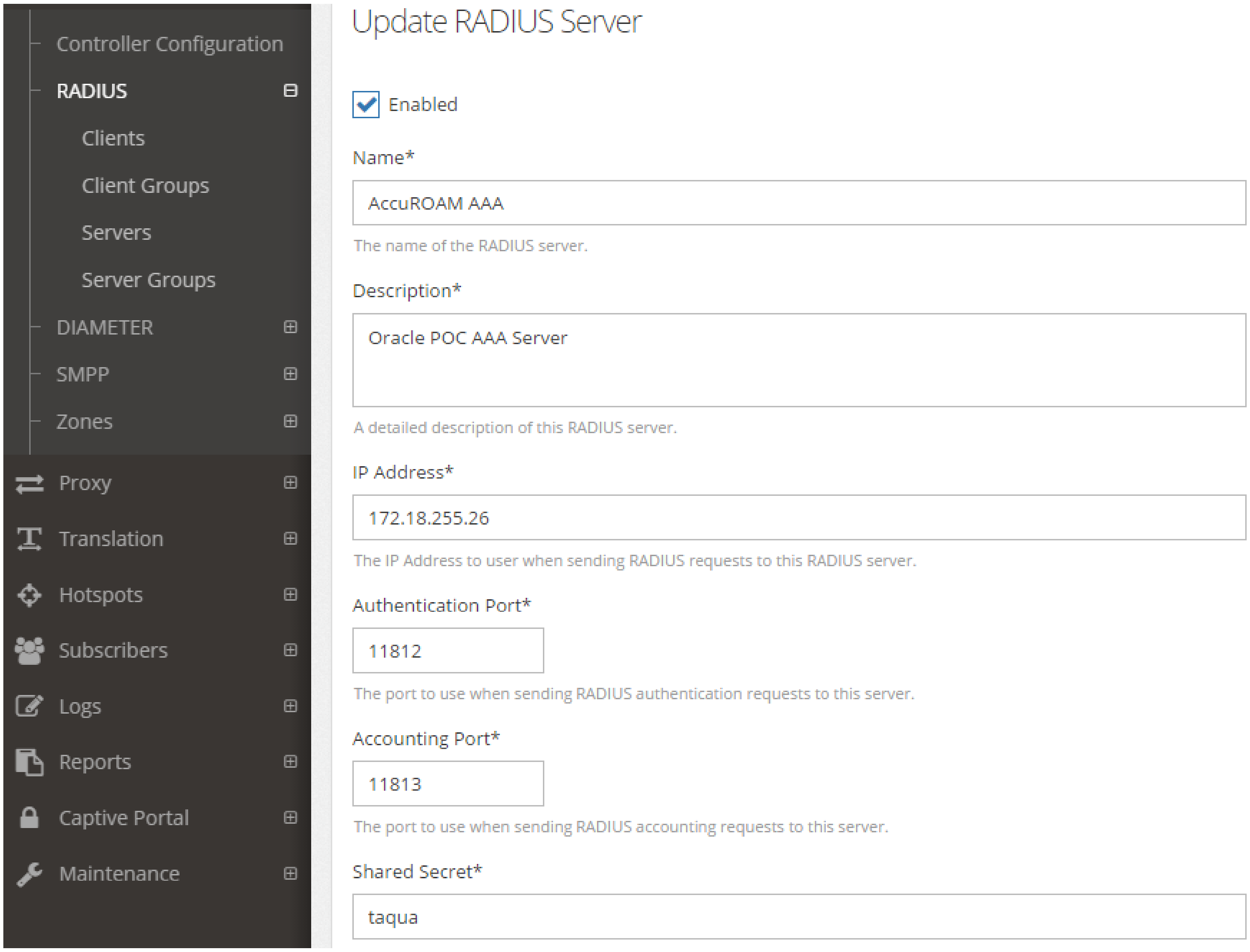
Selected Servers

AccuROAM AAA

The RADIUS Clients that make up this Group. Note: in the case of Primary/Failover the order of the selected list is the order that RADIUS clients are choosen.

Add RADIUS Server (AccuROAM IP address)

To add AccuROAM server IP address, click on RADIUS Server under Network ---- > RADIUS ---- >Servers. Click on **Add New** and create new with the following settings



Update RADIUS Server

☑ Enabled

Name*
AccuROAM AAA
The name of the RADIUS server.

Description*
Oracle POC AAA Server
A detailed description of this RADIUS server.

IP Address*
172.18.255.26
The IP Address to user when sending RADIUS requests to this RADIUS server.

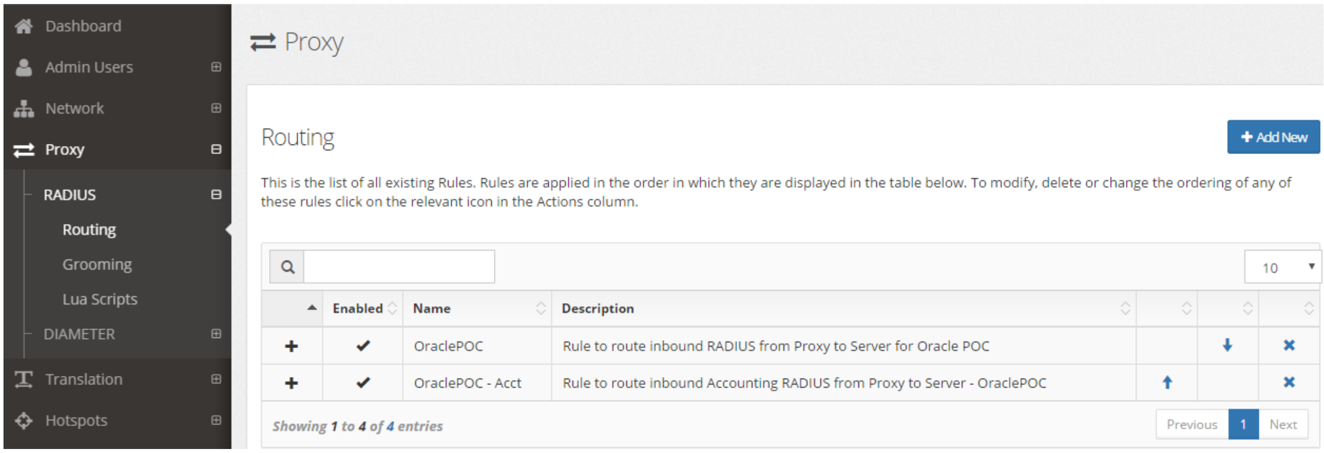
Authentication Port*
11812
The port to use when sending RADIUS authentication requests to this server.

Accounting Port*
11813
The port to use when sending RADIUS accounting requests to this server.

Shared Secret*
taqua

Define Routing

To add route from AAA proxy (internal RADIUS process) to server Proxy --- > RADIUS --- >Routing. Cick on **Add New** and create with the following settings

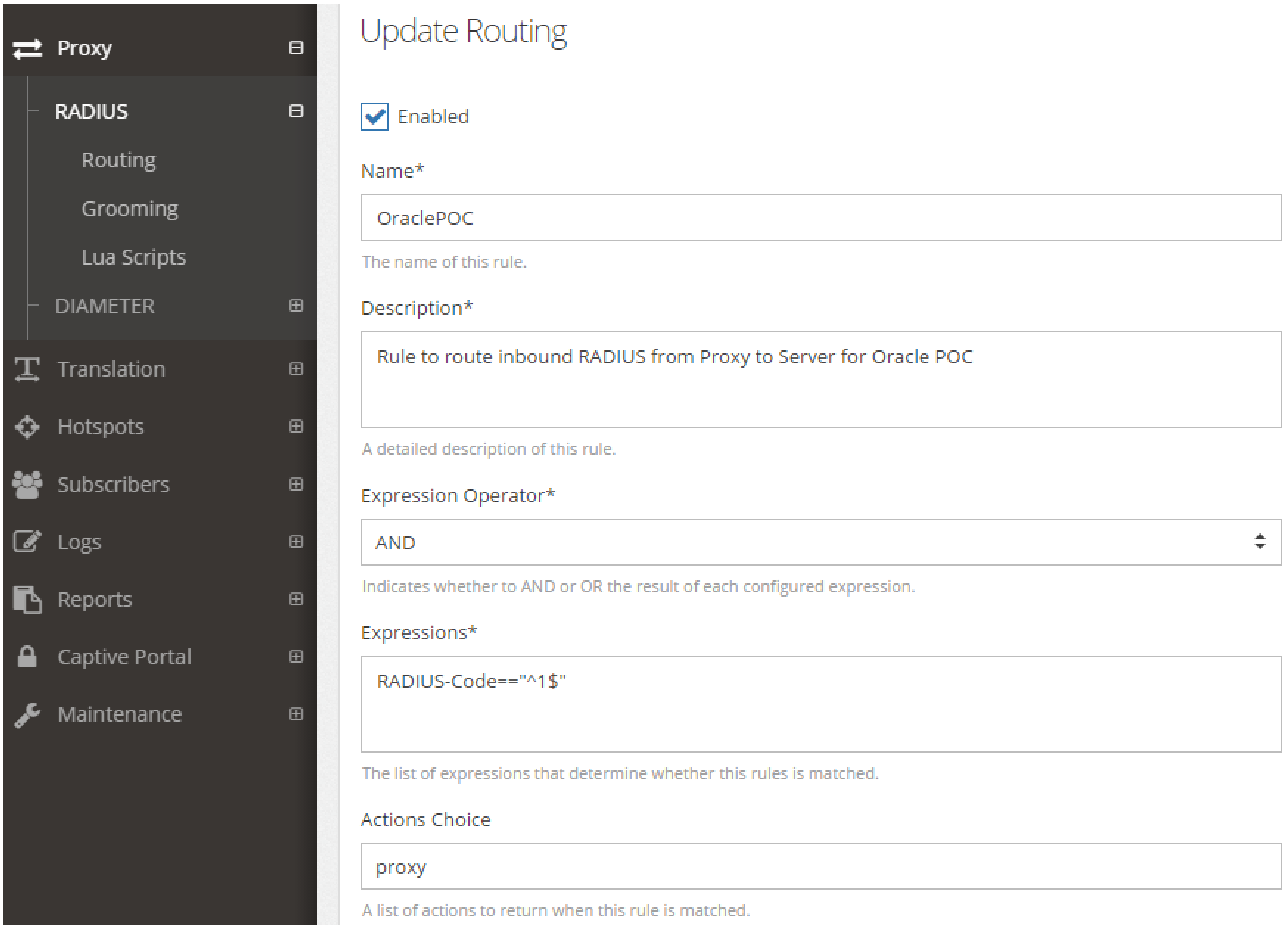


Routing

This is the list of all existing Rules. Rules are applied in the order in which they are displayed in the table below. To modify, delete or change the ordering of any of these rules click on the relevant icon in the Actions column.

	Enabled	Name	Description			
+	✓	OraclePOC	Rule to route inbound RADIUS from Proxy to Server for Oracle POC		↓	✖
+	✓	OraclePOC - Acct	Rule to route inbound Accounting RADIUS from Proxy to Server - OraclePOC	↑		✖

Showing 1 to 4 of 4 entries



Update Routing

☑ Enabled

Name*

OraclePOC

The name of this rule.

Description*

Rule to route inbound RADIUS from Proxy to Server for Oracle POC

A detailed description of this rule.

Expression Operator*

AND

Indicates whether to AND or OR the result of each configured expression.

Expressions*

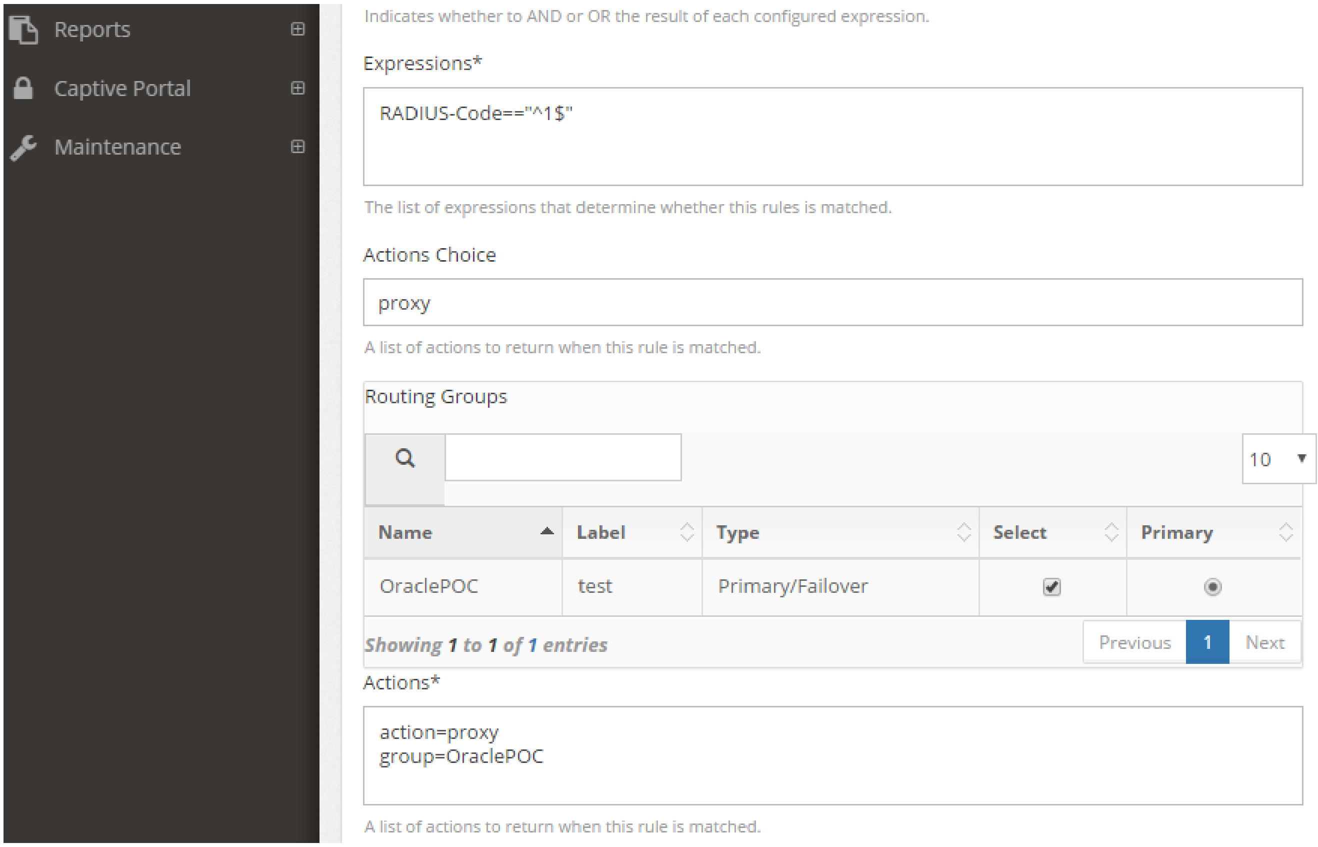
RADIUS-Code=="^1$"

The list of expressions that determine whether this rules is matched.

Actions Choice

proxy

A list of actions to return when this rule is matched.



Indicates whether to AND or OR the result of each configured expression.

Expressions*

```
RADIUS-Code=="^1$"
```

The list of expressions that determine whether this rules is matched.

Actions Choice

proxy

A list of actions to return when this rule is matched.

Routing Groups

10

Name	Label	Type	Select	Primary
OraclePOC	test	Primary/Failover	☑	●

*Showing **1** to **1** of **1** entries*

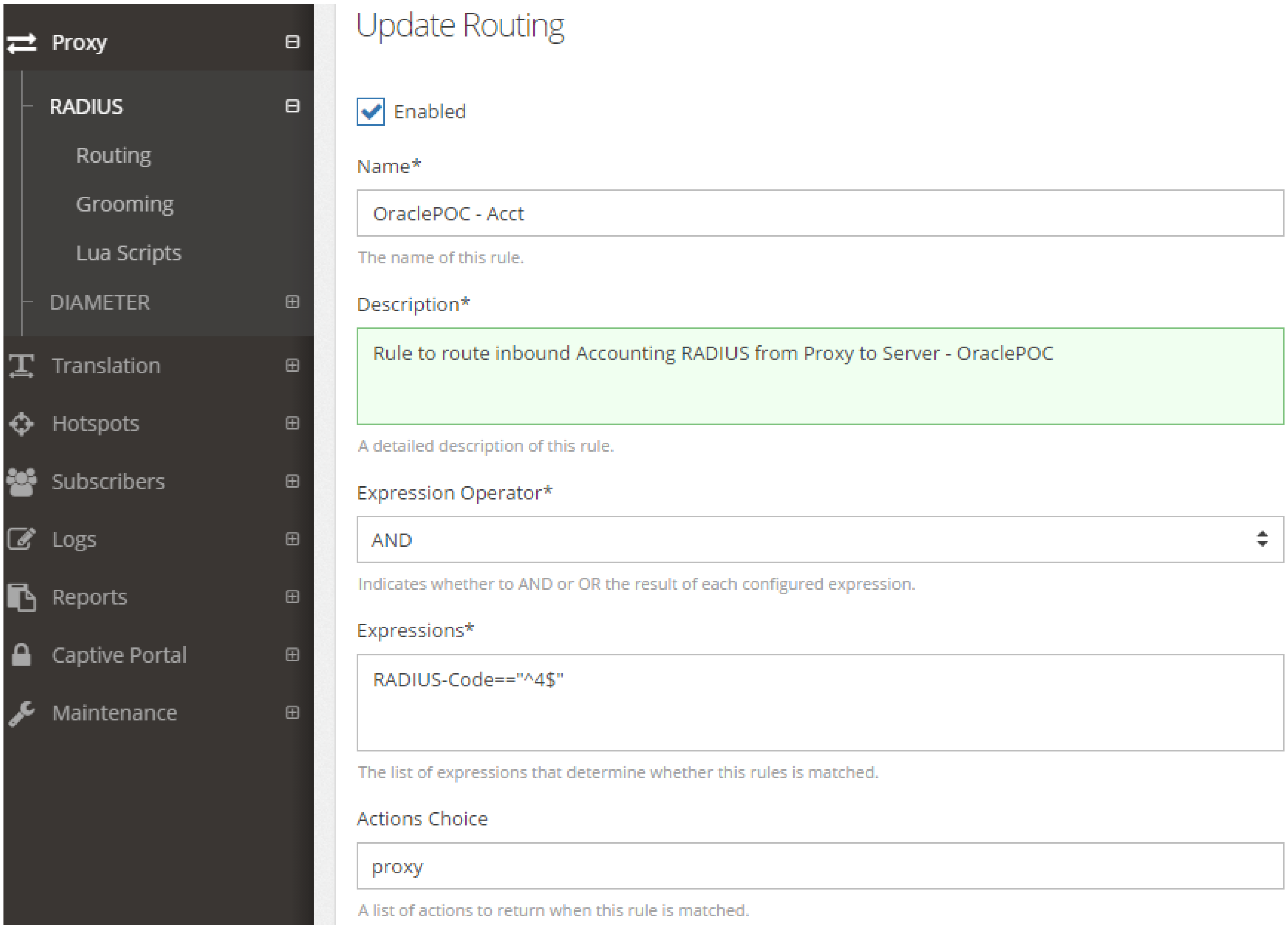
Actions*

```
action=proxy
group=OraclePOC
```

A list of actions to return when this rule is matched.

Configure Accounting Route

Configure route from Accouting proxy internal process to RADIUS accounting server as show below:



Update Routing

☑ Enabled

Name*

OraclePOC - Acct

The name of this rule.

Description*

Rule to route inbound Accounting RADIUS from Proxy to Server - OraclePOC

A detailed description of this rule.

Expression Operator*

AND

Indicates whether to AND or OR the result of each configured expression.

Expressions*

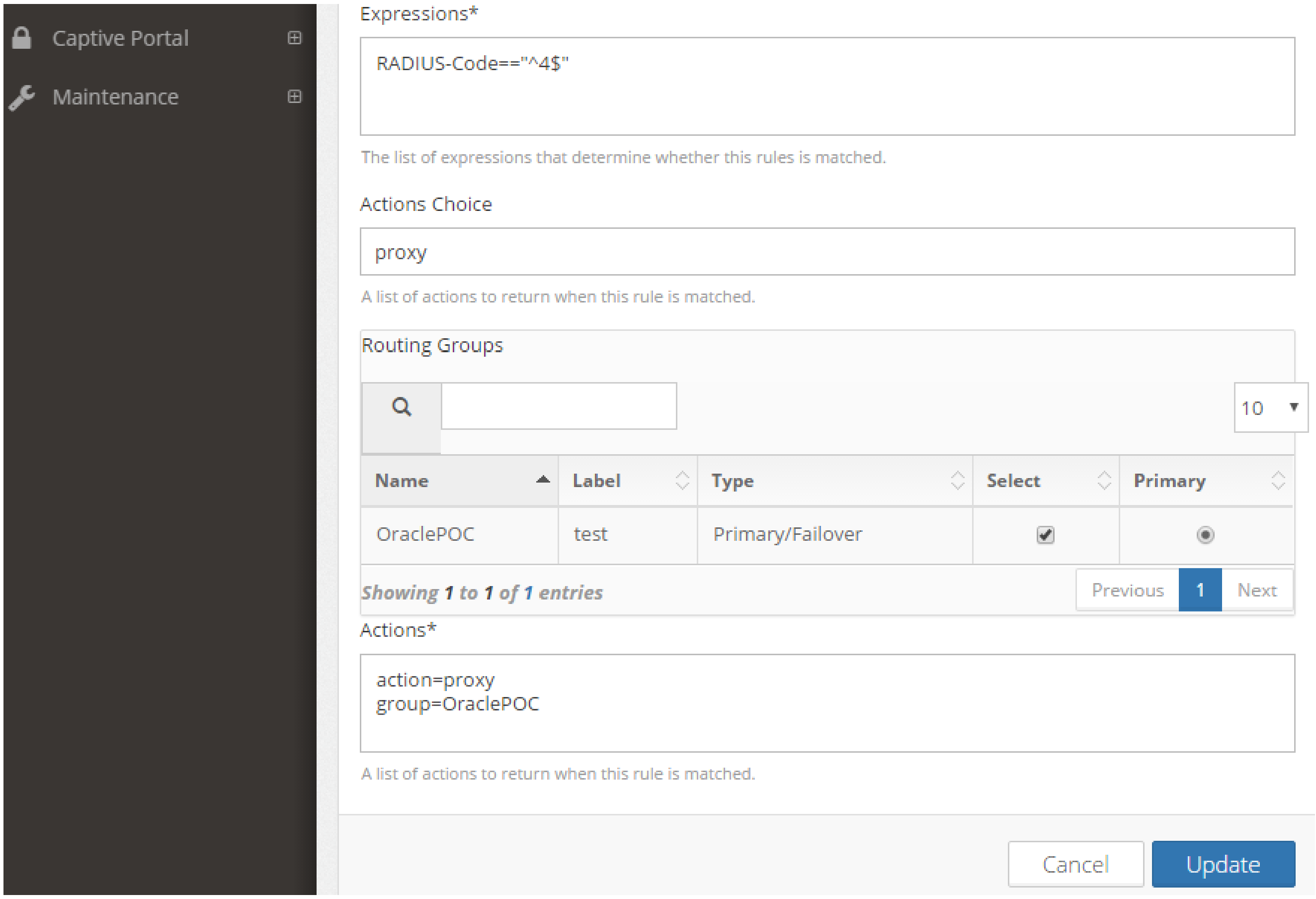
RADIUS-Code=="^4$"

The list of expressions that determine whether this rules is matched.

Actions Choice

proxy

A list of actions to return when this rule is matched.



Expressions*

RADIUS-Code=="^4$"

The list of expressions that determine whether this rules is matched.

Actions Choice

proxy

A list of actions to return when this rule is matched.

Routing Groups

Name	Label	Type	Select	Primary
OraclePOC	test	Primary/Failover	☑	●

*Showing **1** to **1** of **1** entries*

Actions*

```
action=proxy
group=OraclePOC
```

A list of actions to return when this rule is matched.

This completes the configuration on the AccuROAM server. In the troubleshooting section, some pointers are mentioned on starting/stopping processes and capturing traces/logs.

Test Cases Executed

The objective of this integration between Accuris AccuROAM server and Oracle Mobile Security Gateway is to certify the SWm reference point per 3GPP TS 29.273 in a VoWifi architecture.

The following main areas were covered during IOT:

- IPSec tunnel establishment between iPhone 6 and Oracle MSG (interfaction with AccuROAM for device authentication)
- Place VoWifi call once tunnel is established, verify data pass through and tunnel up
- Accounting and Rekeying procedures

Test cases

	Scenario	**Test Case Description**	**Result**
1	**Verify accounting server connectivity**	When MSG comes up, verify Accounting On request/response between MSG and AccuROAM	Pass
2	**Verify Authentication server connectivity**	Verify connectivity on UDP port 1812 with AccuROAM	Pass
3	**IPsec tunnel from UE (authentication)**	Verify UE authentication IPsec tunnel establishment between UE and MSG (interaction with AccuROAM AAA)	Pass
4	**IPsec tunnel tear down when UE roves out of Wi-Fi coverage area**	To test that tunnel delete occurs when UE roves out of Wi-Fi coverage area. Accounting server will be notified.	Pass
5	**Rekeying occurrence**	To test successful rekeying occurrence after device is authenticated. Accounting server will be notified.	Pass
6	**IPsec tunnel reject for barred subscriber**	To test that unauthorized/barred subscriber tunnel attempt is rejected	Pass

Summary

This section provides a statistical summary of the testing.

No. of Test Cases	Pass	Fail	N/S, N/T
6	6	0	0

Conclusions and Recommendations

The integration between Oracle Mobile Security gateway and AccuROAM AAA server has been completed successfully. No open issues reported.

Troubleshooting Tools

This section aims to provide a quick overview on some troubleshooting commands and tips while setting up/verifying IPsec tunnel establishment in the VoWifi environment. It also outlines capturing traces on the AccuROAM server, starting/stopping the processes and viewing logs.

A good area to start troubleshooting when device is not able to setup IPsec tunnel is to look at the message flow in wireshark and output of the IKE and radius statistics from Oracle MSG.

Oracle MSG

The Oracle MSG can be accessed via a SSH session. Following logfiles are notably important when troubleshooting tunnel setup or traffic pass through issues:

- log.iked (for IKEv2 based tunnel establishment)
- log.authd (for radius related exchange)
- log.secured (for IPsec traffic related exchange)

Configuration checklist when IPsec tunnel is failing:

- Check security-policy configuration
- Check ike statistics on the ACLI (show security ike statistics) and radius statistics for EAP exchange (show radius all)
- Ensure connectivity with Internet facing gateway is correct
- Default gateway setting in system-config to be set to outbound/internet facing gateway

The Oracle MSG provides a rich set of statistical counters available from the ACLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces.

Resetting the statistical counters, enabling logging and restarting the log files.

At the MSG Console:

```
VoWifi-MSG# reset iked
VoWifi-MSG# notify iked debug
VoWifi-MSG#
enabled IKE Debugging
VoWifi-MSG# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the MSG with the username user and user mode password (the default is “**acme**”).

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 VoWifi-MSGFTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /opt/logs
250 CWD command successful.
ftp> get log.iked
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/log.iked' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.authd
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/log.authd (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

You may now examine the log files with the text editor of your choice.

The Security gateway essentials guide available at http://docs.oracle.com/cd/E50382_01/doc/sg_mcx300_essentials.pdf explains in greater detail troubleshooting.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org. Wireshark can be installed on a linux server whose interface can be used for port mirroring to capture the IKEv2 and ESP messaging between MSG and iphone (device).

Troubleshooting in AccuROAM Server

The AccROAM server is accessible via SSH as well as the GUI. It has ability to start/stop wireshark capture on all its interfaces, such as RADIUS for authentication, RADIUS for accounting.

The pcaps are available at the following location in AccuROAM:

```
[fmcadm@PROD-1 ~]$ ls -ltr /data_captures/caps/
total 40
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 radius
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 radius_acc
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 m3ua
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 http
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 sip
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 https
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 http_7443
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 ocsp
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 diameter
drwxr-xr-x 3 fmcadm accu 4096 Sep  9  2015 radius_internal
```

Radius and radius_acc directories will contain pcap of the exchange between Oracle MSG and AccuROAM for EAP authentication (radius) and accounting (radius_acc)

Following is the command to start/stop wireshark capture via SSH as user root:

/etc/init.d/startcaps.sh start

/etc/init.d/startcaps.sh stop

Logfiles

Check transaction logs for errors and event logs for alarms/errors. The logs are available at /opt/accu/fmc/log

To list all process running type command ash listprocs. ash startall and ash stopall to start/stop processes.

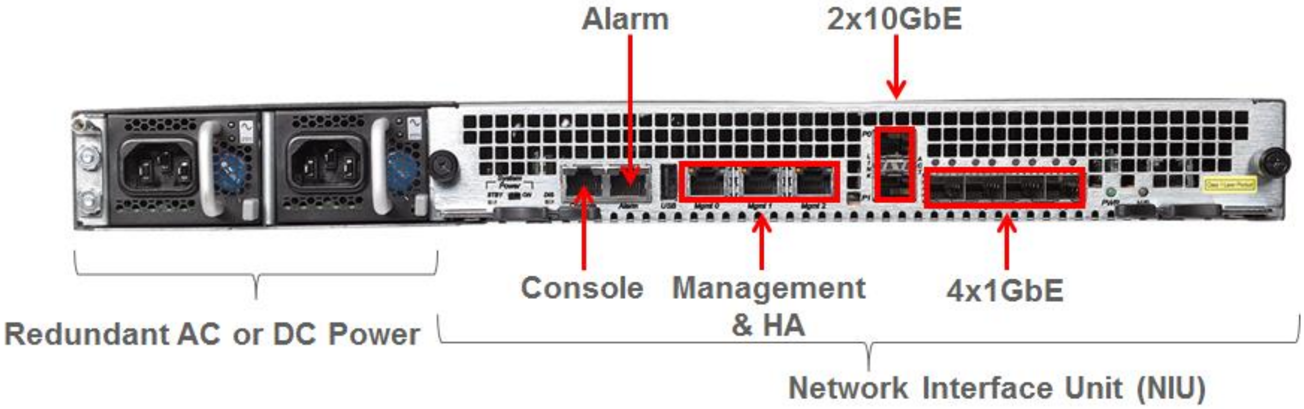
Appendix A

Accessing the MSG ACLI

Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH, this must be explicitly configured.

Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the MSG.

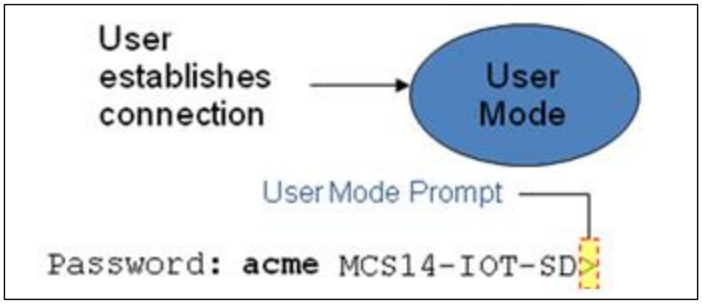


ACLI Basics

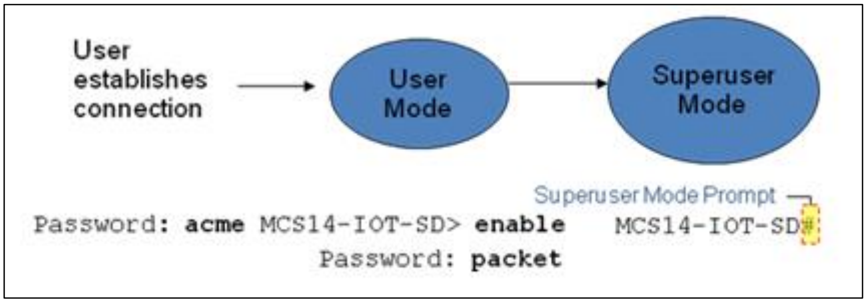
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the MSG, the prompt for the User mode password appears. The default password is acme.

User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



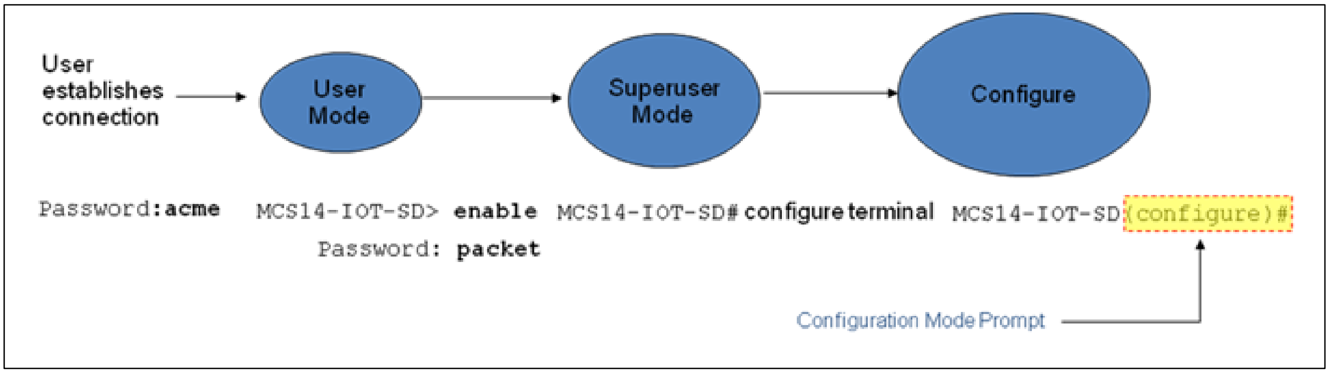
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

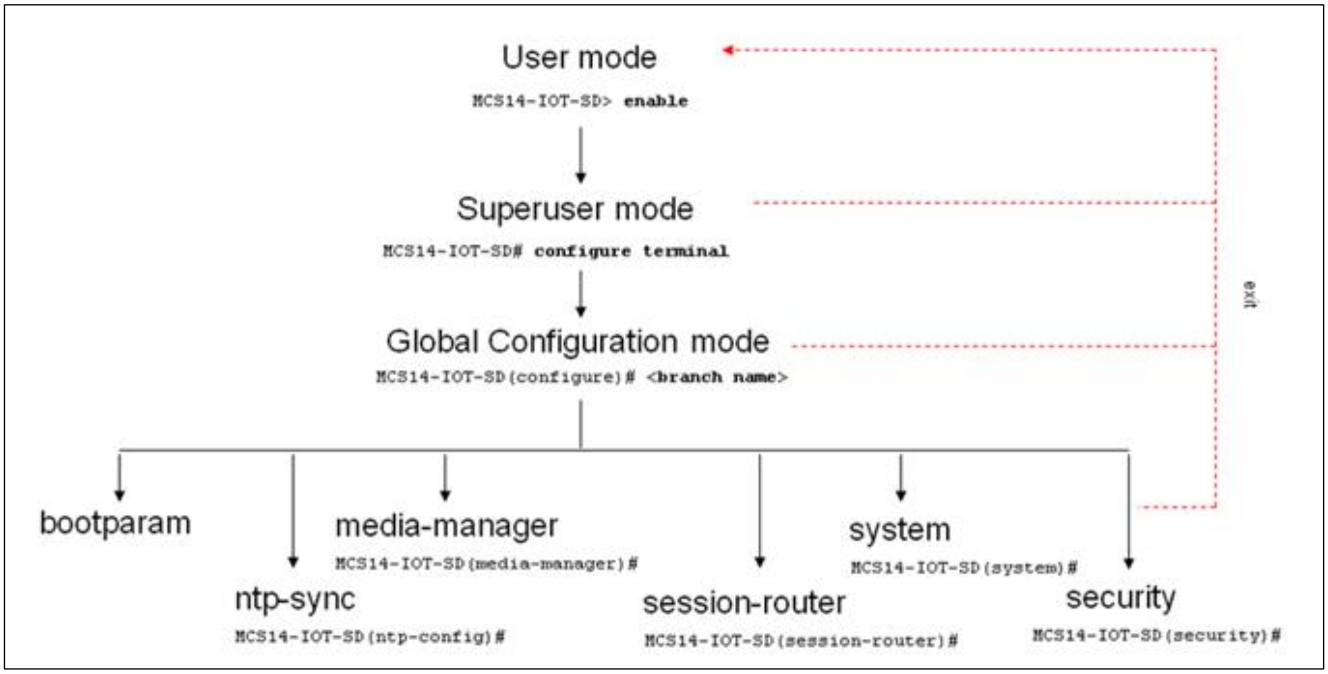
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **VoWifi-MSG(configure)#**. To return to the Superuser mode, issue the **`exit`** command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.


User mode
MCS14-IOT-SD> enable
Superuser mode
MCS14-IOT-SD# configure terminal
Global Configuration mode
MCS14-IOT-SD(configure)# <branch name>
exit
bootparam
media-manager
MCS14-IOT-SD(media-manager)#
system
MCS14-IOT-SD(system)#
ntp-sync
MCS14-IOT-SD(ntp-config)#
session-router
MCS14-IOT-SD(session-router)#
security
MCS14-IOT-SD(security)#

The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to MSG boot parameters. Key boot parameters include:

- boot device – The global management port, usually eth0
- file name – The boot path and the image file.
- inet on ethernet – The IP address and subnet mask (in hex) of the management port of the SD.
- host inet –The IP address of external server where image file resides.
- user and ftp password – Used to boot from the external FTP server.
- gateway inet – The gateway IP address for reaching the external server, if the server is located in a different network.

```
VoWifi-MSG#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device              : eth0
processor number         : 0
host name                : acmesystem
file name                : /code/images/nnMCX300m2p7.tar --- >location
```

```
where the software is loaded on the MSG
inet on ethernet (e)     : 172.18.255.62:ffffff80 --- > This is the ip
address of the management interface of the MSG, type the IP address and
mask in hex
inet on backplane (b)    :
host inet (h)            :
gateway inet (g)         : 172.18.0.1 --- > gateway address here
user (u)                 : vxftp
ftp password (pw) (blank = use rsh)      : vxftp
flags (f)                :
target name (tn)         : VoWifi-MSG
startup script (s)       :
other (o)                :
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the MSG time and date.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The security branch provides access to setting up local-address-pool, ike-interface, ike-config, authentication (for radius server), certificates, security-policy for defining packet treatment, ike-sainfo for defining the encryption and authentication algorithms, etc.

The session-router branch provides access to account-group for defining the radius server

You will use security, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- outbound-sa-fine-grained-mask (child element of security-policy)
- radius-server – in authentication
- account-server – in account-group

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **`show`** command before issuing the **`done`** command. The parameters that you did not configure are filled with either default values or left empty.

4. On completion, you must issue the **`done`** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the **`exit`** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the MSG reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

1. Enter the element that you will edit at the correct level of the ACLI path.
2. Select the element that you will edit, and view it before editing it.
   The **`select`** command loads the element to the volatile memory for editing. The **`show`** command allows you to view the element to ensure that it is the right one that you want to edit.
3. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
4. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the **`show`** command before issuing the **`done`** command.
5. On completion, you must issue the **`done`** command.
6. Issue the **`exit`** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the MSG reboots, your configurations will be lost.

Deleting an Element

The **no** command deletes an element from the configuration in editing.

To delete a single-instance element,

1. Enter the **`no`** command from within the path for that specific element
2. Issue the **`exit`** command.

To delete a multiple-instance element,

1. Enter the **`no`** command from within the path for that particular element.
   The key field prompt, such as <name>:<sub-port-id>, appears.
2. Use the <Enter> key to display a list of the existing configured elements.
3. Enter the number corresponding to the element you wish to delete.
4. Issue the **`select`** command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the MSG reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the MSG: the edited configuration, the saved configuration, and the running configuration.

- The **edited configuration** – this is the version that you are making changes to. This version of the configuration is stored in the system's volatile memory and will be lost on a reboot.
  To view the editing configuration, issue the **`show configuration`** command.

- The **saved configuration –** on issuing the **`save-config`** command, the edited configuration is copied into the non-volatile memory on the system and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The **running configuration** is the saved then activated configuration. On issuing the **`activate-config`** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.
  To view the running configuration, issue command show **`running-config`**.

Saving the Configuration

The **`save-config`** command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the **`save-config`** command, the MSG system displays a reminder on screen stating that you must use the **`activate-config`** command if you want the configurations to be updated.

```
VoWifi-MSG# save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
VoWifi-MSG#
```

Activating the Configuration

On issuing the **`activate-config`** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the MSG warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
VoWifi-MSG# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
VoWifi-MSG#
```

Appendix – B: Sample Configuration from Oracle Mobile Security Gateway

```
VoWiFi-MSG# show running-config
account-group
        name                                    AccuRoam
        hostname                                localhost
        acct-protocol                           RADIUS
        acct-src-port                           1813
        acct-strategy                           Hunt
        account-servers
                hostname                                10.20.30.45
                port                                    1813
                state                                   enabled
                min-round-trip                          250
                max-inactivity                          60
                restart-delay                           30
                bundle-vsa                              enabled
                secret                                  ********
                NAS-ID                                  Oracle-SG
                priority                                0
                origin-realm
                domain-name-suffix
                watchdog-ka-timer                       0
                diameter-in-manip
                diameter-out-manip
        options
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-10-01 14:53:28
auth-params
        name                                    tradius
        protocol                                eap
        strategy                                hunt
        servers                                 10.20.30.45
        authorization-servers
        options
        last-modified-by                        admin@172.18.0.149
        last-modified-date                      2015-09-23 18:10:59
authentication
        source-port                             1812
        type                                    radius
        protocol                                pap
        tacacs-authorization                    enabled
        tacacs-accounting                       enabled
        server-assigned-privilege               disabled
        allow-local-authorization               disabled
        login-as-admin                          disabled
        management-strategy                     hunt
        ike-radius-params-name                  tradius
        management-servers                      10.20.30.45
        radius-server
                address                                 10.20.30.45
                port                                    1812
                state                                   enabled
                secret                                  ********
                nas-id                                  taqua
                realm-id
                retry-limit                             3
                retry-time                              5
                maximum-sessions                        255
                class                                   primary
                dead-time                               10
                authentication-methods                  all
        last-modified-by                        admin@172.18.0.149
        last-modified-date                      2015-09-23 18:10:42
certificate-record
        name                                    ello_client_cert
        country                                 US
        state                                   TX
        locality                                Taqua Lab
        organization                            Engineering
        unit
        common-name                             Ello Cloud
        key-size                                1024
        alternate-name
DNS:osegw.ellocloud.net,IP:64.201.141.84
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        cert-status-profile-list
        options
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-19 14:37:13
certificate-record
        name                                    ello_root_cert
        country                                 US
        state                                   TX
        locality                                Taqua Lab
        organization                            Ello Cloud
        unit
        common-name                             Ello Cloud Certificate
Signing Authority
        key-size                                1024
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        cert-status-profile-list
        options
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-23 17:48:51
certificate-record
        name                                    msg_cert
        country                                 US
        state                                   MA
        locality                                Burlington
        organization                            Engineering
        unit
        common-name                             64.201.141.84
        key-size                                1024
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        cert-status-profile-list
        options
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-18 15:07:43
certificate-record
        name                                    root_cert
        country                                 US
        state                                   MA
        locality                                Burlington
        organization                            Engineering
        unit
        common-name                             selab-DOMAINCONTROL-CA
        key-size                                1024
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        cert-status-profile-list
        options
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-18 15:08:10
data-flow
        name                                    data-flow
        realm-id                                core
        group-size                              128
        upstream-rate                           0
        downstream-rate                         0
        last-modified-by                        admin@172.18.0.164
        last-modified-date                      2014-09-23 18:45:49
dpd-params
        name                                    dpd-SG
        max-loop                                100
        max-endpoints                           25
        max-cpu-limit                           60
        load-max-loop                           40
        load-max-endpoints                      5
        max-attempts                            1
        max-retrans                             3
        last-modified-by                        admin@172.18.0.145
        last-modified-date                      2015-08-17 17:30:32
ike-accounting-param
        name                                    Accu-accounting
        radius-accounting-events                start
                                                stop
                                                interim_ipsec_rekey
                                                interim_ike_rekey
        diameter-accounting-events
        intermediate-period                     0
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-10-01 14:49:10
ike-certificate-profile
        identity                                osegw.ellocloud.net
        end-entity-certificate                  ello_client_cert
        trusted-ca-certificates                 ello_root_cert
        verify-depth                            3
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-23 17:44:12
ike-config
        state                                   enabled
        ike-version                             2
        log-level                               DEBUG
        udp-port                                500
        negotiation-timeout                     15
        event-timeout                           60
        phase1-mode                             main
        phase1-dh-mode                          first-supported
        v2-ike-life-secs                        86400
        v2-ipsec-life-secs                      28800
        v2-rekey                                disabled
        anti-replay                             enabled
        phase1-life-seconds                     3600
        phase1-life-secs-max                    86400
        phase2-life-seconds                     28800
        phase2-life-secs-max                    86400
        phase2-exchange-mode                    phase1-group
        shared-password                         ********
        eap-protocol                            eap-radius-passthru
        eap-bypass-identity                     disabled
        addr-assignment                         local
        dpd-time-interval                       60
        overload-threshold                      100
        overload-interval                       1
        overload-action                         none
        overload-critical-threshold             100
        overload-critical-interval              1
        red-port                                0
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        sd-authentication-method                certificate
        certificate-profile-id                  osegw.ellocloud.net
        id-auth-type                            idi
        options                                 assume-initial-contact
                                                triple-des-zero
        account-group-list
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-09-11 21:19:18
ike-interface
        state                                   enabled
        address                                 168.212.244.150
        realm-id                                public
        ike-mode                                responder
        dpd-params-name                         dpd-SG
        v2-ike-life-secs                        82800
        v2-ipsec-life-secs                      600
        v2-rekey                                enabled
        multiple-authentication                 disabled
        multiple-child-sa-mode                  none
        shared-password                         ********
        options
        eap-protocol                            eap-radius-passthru
        sd-authentication-method                certificate
        certificate-profile-id-list             osegw.ellocloud.net
        threshold-crossing-alert-group-name
        cert-status-check                       disabled
        cert-status-profile-list
        access-control-name
        traffic-selectors
        ip-subnets
        authorization                           disabled
        tunnel-orig-name-list
        security-interface-params-name          ike-vowifi
        last-modified-by                        admin@172.18.0.145
        last-modified-date                      2015-10-02 15:51:41
ike-sainfo
        name                                    ike-sainfo
        security-protocol                       esp-auth
        auth-algo                               any
        encryption-algo                         aes
        ipsec-mode                              tunnel
        tunnel-local-addr                       168.212.244.150
        tunnel-remote-addr                      *
        last-modified-by                        admin@172.18.0.158
        last-modified-date                      2015-07-17 15:26:50
ipsec-global-config
        red-ipsec-port                          0
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        options                                 fragmented-packet-allow
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-31 11:54:40
local-address-pool
        name                                    addr-pool
        address-range
                network-address                         10.10.10.0
                subnet-mask                             255.255.255.0
                gateway
        dns-realm-id                            core
        data-flow                               data-flow
        dns-assignment
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2015-03-31 11:54:18
media-manager
        state                                   enabled
        latching                                enabled
        flow-time-limit                         86400
        initial-guard-timer                     300
        subsq-guard-timer                       300
        tcp-flow-time-limit                     86400
        tcp-initial-guard-timer                 300
        tcp-subsq-guard-timer                   300
        tcp-number-of-ports-per-flow            2
        hnt-rtcp                                disabled
        algd-log-level                          NOTICE
        mbcd-log-level                          NOTICE
        options
        red-flow-port                           1985
        red-mgcp-port                           1986
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        media-policing                          enabled
        max-signaling-bandwidth                 10000000
        max-untrusted-signaling                 100
        min-untrusted-signaling                 30
        tolerance-window                        30
        trap-on-demote-to-deny                  disabled
        trap-on-demote-to-untrusted             disabled
        syslog-on-demote-to-deny                disabled
        syslog-on-demote-to-untrusted           disabled
        rtcp-rate-limit                         0
        anonymous-sdp                           disabled
        arp-msg-bandwidth                       32000
        rfc2833-timestamp                       disabled
        default-2833-duration                   100
        rfc2833-end-pkts-only-for-non-sig       enabled
        translate-non-rfc2833-event             disabled
        media-supervision-traps                 disabled
        dnsalg-server-failover                  disabled
        syslog-on-call-reject                   disabled
        last-modified-by                        admin@172.18.0.119
        last-modified-date                      2014-10-07 16:38:12
network-interface
        name                                    s0p4
        sub-port-id                             0
        description
        hostname
        ip-address                              168.212.244.150
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 168.212.244.1
        sec-gateway
        gw-heartbeat
                state                                   disabled
                heartbeat                               0
                retry-count                             0
                retry-timeout                           1
                health-score                            0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                             11
        signaling-mtu                           0
        hip-ip-list                             168.212.244.150
        ftp-address
        icmp-address                            168.212.244.150
        snmp-address
        telnet-address
        ssh-address                             168.212.244.150
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:20:26
network-interface
        name                                    s0p5
        sub-port-id                             0
        description
        hostname
        ip-address                              192.168.1.120
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 192.168.1.105
        sec-gateway
        gw-heartbeat
                state                                   enabled
                heartbeat                               10
                retry-count                             3
                retry-timeout                           1
                health-score                            25
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                             11
        signaling-mtu                           0
        hip-ip-list                             192.168.1.120
        ftp-address
        icmp-address                            192.168.1.120
        snmp-address
        telnet-address
        ssh-address                             192.168.1.120
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:20:33
phy-interface
        name                                    s0p4
        operation-type                          Media
        port                                    4
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        disabled
        duplex-mode
        speed
        wancom-health-score                     50
        overload-protection                     disabled
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:19:53
phy-interface
        name                                    s0p5
        operation-type                          Media
        port                                    5
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode
        speed
        wancom-health-score                     50
        overload-protection                     disabled
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:20:15
realm-config
        identifier                              core
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p5:0
        mm-in-realm                             enabled
        mm-in-network                           enabled
        mm-same-ip                              enabled
        mm-in-system                            enabled
        bw-cac-non-mm                           disabled
        msm-release                             disabled
        qos-enable                              disabled
        max-bandwidth                           0
        fallback-bandwidth                      0
        max-priority-bandwidth                  0
        max-latency                             0
        max-jitter                              0
        max-packet-loss                         0
        observ-window-size                      0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough                    disabled
        class-profile
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        average-rate-limit                      0
        access-control-trust-level              none
        invalid-signal-threshold                0
        maximum-signal-threshold                0
        untrusted-signal-threshold              0
        nat-trust-threshold                     0
        max-endpoints-per-nat                   0
        nat-invalid-message-threshold           0
        wait-time-for-invalid-register          0
        deny-period                             30
        cac-failure-threshold                   0
        untrust-cac-failure-threshold           0
        ext-policy-svr
        diam-e2-address-realm
        subscription-id-type                    END_USER_NONE
        symmetric-latching                      disabled
        pai-strip                               disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching                     none
        restriction-mask                        32
        user-cac-mode                           none
        user-cac-bandwidth                      0
        user-cac-sessions                       0
        icmp-detect-multiplier                  0
        icmp-advertisement-interval             0
        icmp-target-ip
        monthly-minutes                         0
        options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        refer-notify-provisional                none
        dyn-refer-term                          disabled
        codec-policy
        codec-manip-in-realm                    disabled
        codec-manip-in-network                  enabled
        rtcp-policy
        constraint-name
        call-recording-server-id
        session-recording-server
        session-recording-required              disabled
        manipulation-string
        manipulation-pattern
        stun-enable                             disabled
        stun-server-ip                          0.0.0.0
        stun-server-port                        3478
        stun-changed-ip                         0.0.0.0
        stun-changed-port                       3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                              disabled
        hide-egress-media-update                disabled
        tcp-media-profile
        monitoring-filters
        node-functionality
        default-location-string
        alt-family-realm
        pref-addr-type                          none
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:21:01
realm-config
        identifier                              public
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p4:0
        mm-in-realm                             enabled
        mm-in-network                           enabled
        mm-same-ip                              enabled
        mm-in-system                            enabled
        bw-cac-non-mm                           disabled
        msm-release                             disabled
        qos-enable                              disabled
        max-bandwidth                           0
        fallback-bandwidth                      0
        max-priority-bandwidth                  0
        max-latency                             0
        max-jitter                              0
        max-packet-loss                         0
        observ-window-size                      0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough                    disabled
        class-profile
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        average-rate-limit                      0
        access-control-trust-level              none
        invalid-signal-threshold                0
        maximum-signal-threshold                0
        untrusted-signal-threshold              0
        nat-trust-threshold                     0
        max-endpoints-per-nat                   0
        nat-invalid-message-threshold           0
        wait-time-for-invalid-register          0
        deny-period                             30
        cac-failure-threshold                   0
        untrust-cac-failure-threshold           0
        ext-policy-svr
        diam-e2-address-realm
        subscription-id-type                    END_USER_NONE
        symmetric-latching                      disabled
        pai-strip                               disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching                     none
        restriction-mask                        32
        user-cac-mode                           none
        user-cac-bandwidth                      0
        user-cac-sessions                       0
        icmp-detect-multiplier                  0
        icmp-advertisement-interval             0
        icmp-target-ip
        monthly-minutes                         0
        options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        refer-notify-provisional                none
        dyn-refer-term                          disabled
        codec-policy
        codec-manip-in-realm                    disabled
        codec-manip-in-network                  enabled
        rtcp-policy
        constraint-name
        call-recording-server-id
        session-recording-server
        session-recording-required              disabled
        manipulation-string
        manipulation-pattern
        stun-enable                             disabled
        stun-server-ip                          0.0.0.0
        stun-server-port                        3478
        stun-changed-ip                         0.0.0.0
        stun-changed-port                       3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                              disabled
        hide-egress-media-update                disabled
        tcp-media-profile
        monitoring-filters
        node-functionality
        default-location-string
        alt-family-realm
        pref-addr-type                          none
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-09-04 17:21:13
security-interface-params
        identifier                              ike-vowifi
        address-assignment                      local
        authentication-servers                  10.20.30.45
        authorization-servers
        accounting-params-name                  Accu-accounting
        account-group-list                      AccuRoam
        local-address-pool-id-list              addr-pool
        sg-policy-list
        options
        last-modified-by                        admin@172.18.0.115
        last-modified-date                      2015-10-01 14:54:12
security-policy
        name                                    allow-esp
        network-interface                       s0p5:0
        priority                                101
        local-ip-addr-match                     0.0.0.0
        remote-ip-addr-match                    0.0.0.0
        local-port-match                        0
        local-port-match-max                    65535
        remote-port-match                       0
        remote-port-match-max                   65535
        trans-protocol-match                    ALL
        trans-sub-protocol-match                50
        trans-sub-protocol-code-match           4294967295
        direction                               both
        local-ip-mask                           0.0.0.0
        remote-ip-mask                          0.0.0.0
        action                                  allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                           255.255.255.255
                remote-ip-mask                          255.255.255.255
                local-port-mask                         0
                remote-port-mask                        0
                trans-protocol-mask                     0
                valid                                   enabled
                vlan-mask                               0x000
        last-modified-by                        admin@172.18.0.103
        last-modified-date                      2015-09-22 17:18:45
security-policy
        name                                    ipsec-policy
        network-interface                       s0p4:0
        priority                                11
        local-ip-addr-match                     0.0.0.0
        remote-ip-addr-match                    10.10.10.0
        local-port-match                        0
        local-port-match-max                    65535
        remote-port-match                       0
        remote-port-match-max                   65535
        trans-protocol-match                    ALL
        trans-sub-protocol-match                4294967295
        trans-sub-protocol-code-match           4294967295
        direction                               both
        local-ip-mask                           0.0.0.0
        remote-ip-mask                          255.255.255.0
        action                                  ipsec
        ike-sainfo-name                         ike-sainfo
        outbound-sa-fine-grained-mask
                local-ip-mask                           0.0.0.0
                remote-ip-mask                          255.255.255.255
                local-port-mask                         0
                remote-port-mask                        0
                trans-protocol-mask                     0
                valid                                   enabled
                vlan-mask                               0x000
        last-modified-by                        admin@172.18.0.103
        last-modified-date                      2015-09-22 17:19:18
security-policy
        name                                    sec-policy
        network-interface                       s0p4:0
        priority                                0
        local-ip-addr-match                     168.212.244.150
        remote-ip-addr-match                    0.0.0.0
        local-port-match                        500
        local-port-match-max                    65535
        remote-port-match                       0
        remote-port-match-max                   65535
        trans-protocol-match                    ALL
        trans-sub-protocol-match                4294967295
        trans-sub-protocol-code-match           4294967295
        direction                               both
        local-ip-mask                           255.255.255.255
        remote-ip-mask                          0.0.0.0
        action                                  allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                           0.0.0.0
                remote-ip-mask                          0.0.0.0
                local-port-mask                         0
                remote-port-mask                        0
                trans-protocol-mask                     0
                valid                                   enabled
                vlan-mask                               0x000
        last-modified-by                        admin@172.18.0.103
        last-modified-date                      2015-09-22 17:04:42
security-policy
        name                                    sec-policy-nat
        network-interface                       s0p4:0
        priority                                10
        local-ip-addr-match                     168.212.244.150
        remote-ip-addr-match                    0.0.0.0
        local-port-match                        4500
        local-port-match-max                    65535
        remote-port-match                       0
        remote-port-match-max                   65535
        trans-protocol-match                    ALL
        trans-sub-protocol-match                4294967295
        trans-sub-protocol-code-match           4294967295
        direction                               both
        local-ip-mask                           255.255.255.255
        remote-ip-mask                          0.0.0.0
        action                                  allow
        ike-sainfo-name
        outbound-sa-fine-grained-mask
                local-ip-mask                           255.255.255.255
                remote-ip-mask                          255.255.255.255
                local-port-mask                         0
                remote-port-mask                        0
                trans-protocol-mask                     0
                valid                                   enabled
                vlan-mask                               0x000
        last-modified-by                        admin@172.18.0.103
        last-modified-date                      2015-09-22 17:19:33
steering-pool
        ip-address                              168.212.244.150
        start-port                              10000
        end-port                                10500
        realm-id                                public
        network-interface
        last-modified-by                        admin@172.18.0.158
        last-modified-date                      2015-07-17 15:24:00
steering-pool
        ip-address                              192.168.1.120
        start-port                              10500
        end-port                                20000
        realm-id                                core
        network-interface
        last-modified-by                        admin@172.18.0.118
        last-modified-date                      2015-07-23 14:59:14
system-config
        hostname
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                            enabled
        enable-snmp-auth-traps                  disabled
        enable-snmp-syslog-notify               disabled
        enable-snmp-monitor-traps               disabled
        enable-env-monitor-traps                disabled
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        system-log-level                        WARNING
        process-log-level                       WARNING
        process-log-ip-address                  0.0.0.0
        process-log-port                        0
        collect
                sample-interval                         5
                push-interval                           15
                boot-state                              disabled
                start-time                              now
                end-time                                never
                red-collect-state                       disabled
                red-max-trans                           1000
                red-sync-start-time                     5000
                red-sync-comp-time                      1000
                push-success-trap-state                 disabled
        call-trace                              disabled
        internal-trace                          disabled
        log-filter                              all
        default-gateway                         168.212.244.1
        restart                                 enabled
        exceptions
        telnet-timeout                          0
        console-timeout                         0
        remote-control                          enabled
        cli-audit-trail                         enabled
        link-redundancy-state                   disabled
        source-routing                          disabled
        cli-more                                disabled
        terminal-height                         24
        debug-timeout                           0
        trap-event-lifetime                     0
        ids-syslog-facility                     -1
        options
        default-v6-gateway                      ::
        ipv6-signaling-mtu                      1500
        ipv4-signaling-mtu                      1500
        cleanup-time-of-day                     00:00
        snmp-engine-id-suffix
        snmp-agent-mode                         v1v2
```

Appendix C – Oracle Communications MSG SW 3.0 highlights

This section highlights some of the important additions and feature inclusions in Oracle Communications security gateway SW 3.0 and the hardware requisite. (For detailed features and description, please review the Oracle Communications Security gateway MC-X 3.0 Essentials Guide)

The Oracle Communications 4500 platform running MSG SW 3.0 latest GA can be used for VoWifi application for existing customers for the short term as temporary solution, although it is highly recommended to upgrade to the 4600/6100/6300 platforms with MCZ 4.0 software to avail of the improved platform strength and features such as integration with EPC networks. Below are the subtle differences in configuration on SW 3.0 when defining the AccuROAM server for authentication and accounting.

Configuration highlights in SW 3.0

The MSG configuration follows in general a security gateway configuration per the concepts outlined in the security gatway essentials guide available at http://docs.oracle.com/cd/E50382_01/doc/sg_mcx300_essentials.pdf . Note, there is no security-interface-params element in SW 3.0 (as found in SW 4.0). Ike-interface and ike-config containers have provision to reference authentication and accounting server information.

Authentication and Accounting

To define the AccuROAM server for authentication and accounting, following steps are required:

- Define Authentication element and reference the IP address of the AccuROAM server
- Define auth-params element
- Define account-group element and configure IP address of AccuROAM for accounting
- Define Ike-accounting-param and choose type of accounting records
- Reference accounting-param name and authentication server in ike-interface
- Reference account-group (radius server) in ike-config

Authentication

We define an authentication element in the security configuration to define the AccuROAM server and configure the secret (password) as show below:

```
authentication
        source-port                    1812
        type                           radius
        protocol                       pap
        allow-local-authorization      disabled
        login-as-admin                 disabled
        management-strategy            hunt
        ike-radius-params-name         tradius
        management-servers
                                       10.20.30.45
        radius-server
                address                        10.20.30.45
                port                           1812
                state                          enabled
                secret                         <key value encrypted, not
shown>
                nas-id                         taqua
                realm-id
                retry-limit                    3
                retry-time                     5
                maximum-sessions               255
                class                          primary
                dead-time                      10
                authentication-methods
                                               all
```

Auth-params

Define the authentication server in auth-params under configure terminal --- > security ---- > auth-params

```
auth-params
        name                           tradius
        protocol                       eap
        strategy                       hunt
        servers
                                       10.20.30.45
        authorization-servers
```

Account-group

Configure an account-group for adding accouting server with secret/password under configure terminal --- > account-group

```
account-group
        name                           AccuROAM
        hostname                       localhost
        protocol                       RADIUS
        src-port                       1813
        strategy                       Hunt
        account-server
                hostname                       10.20.30.45
                port                           1813
                state                          enabled
                min-round-trip                 250
                max-inactivity                 60
                restart-delay                  30
                bundle-vsa                     enabled
                secret                         <key value encrypted, not
shown>
                NAS-ID                         Oracle-4500-SG
                priority                       0
                origin-realm
                domain-name-suffix
```

Ike-accounting-param

Configure ike-accounting-param and choose the type of accounting records you want system to send to AAA server

```
ike-accounting-param
        name                           Accu-accounting
        radius-accounting-events       start stop interim_ipsec_rekey
interim_ike_rekey
        diameter-accounting-events
        intermediate-period            0
```

Update accounting-param and authentication server in Ike-interface

```
ike-interface
        state                          enabled
        address                        168.212.244.150
        realm-id                       public
        ike-mode                       responder
        local-address-pool-id-list     addr-pool
        dpd-params-name                dpd-SG
        v2-ike-life-secs               82800
        v2-ipsec-life-secs             600
        v2-rekey                       enabled
        multiple-authentication        disabled
        multiple-child-sa-mode         none
        shared-password                <key value encrypted, not shown>
        eap-protocol                   eap-radius-passthru
        addr-assignment                local
        sd-authentication-method       certificate
        certificate-profile-id-list    osegw.ellocloud.net
        threshold-crossing-alert-group-name
        cert-status-check              disabled
        cert-status-profile-list
        access-control-name
        accounting-param-name          Accu-accounting
        traffic-selectors
        ip-subnets
        authorization                  disabled
        tunnel-orig-name-list
        authentication-servers         10.20.30.45
        authorization-servers
```

Reference account-group server (radius server) in ike-interface under account-group-list sub-element

```
ike-config
        state                          enabled
        ike-version                    2
        log-level                      DEBUG
        udp-port                       500
        negotiation-timeout            15
        event-timeout                  60
        phase1-mode                    main
        phase1-dh-mode                 first-supported
        v2-ike-life-secs               86400
        v2-ipsec-life-secs             28800
        v2-rekey                       disabled
        anti-replay                    enabled
        phase1-life-seconds            3600
        phase1-life-secs-max           86400
        phase2-life-seconds            28800
        phase2-life-secs-max           86400
        phase2-exchange-mode           phase1-group
        shared-password                <key value encrypted, not shown>
        eap-protocol                   eap-radius-passthru
        eap-bypass-identity            disabled
        addr-assignment                local
        dpd-time-interval              60
        overload-threshold             100
        overload-interval              1
        overload-action                none
        overload-critical-threshold    100
        overload-critical-interval     1
        red-port                       0
```

```
         red-max-trans                  10000
         red-sync-start-time            5000
         red-sync-comp-time             1000
         sd-authentication-method       certificate
         certificate-profile-id         osegw.ellocloud.net
         id-auth-type                   idi
         options                        assume-initial-contact
                                        triple-des-zero
         account-group-list             AccuRoam
```

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services