ORACLE COMMUNICATIONS

Oracle Enterprise Session Border Controller Line-Side with Avaya Aura 6.3 and 7.0 with the Oracle Enterprise Operations Monitor

Technical Application Note

ORACLE

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 is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Communications Enterprise-SBC, Oracle Enterprise Operations Monitor, and Avaya Aura Session Manager. There will be steps that require navigating the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Document Overview

This technical application note documents the implementation of the Oracle Enterprise Session Border Controller (E-SBC) line-side between Avaya endpoints (hard phones and soft clients) and the Avaya Aura Session Manager (SM).

It should be noted that the E-SBC configuration provided in this guide focuses strictly on the Avaya SM, phone, and client associated parameters. Many E-SBC users may have additional configuration requirements that are specific to other applications. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Introduction

Enterprise Session Border Controller Overview

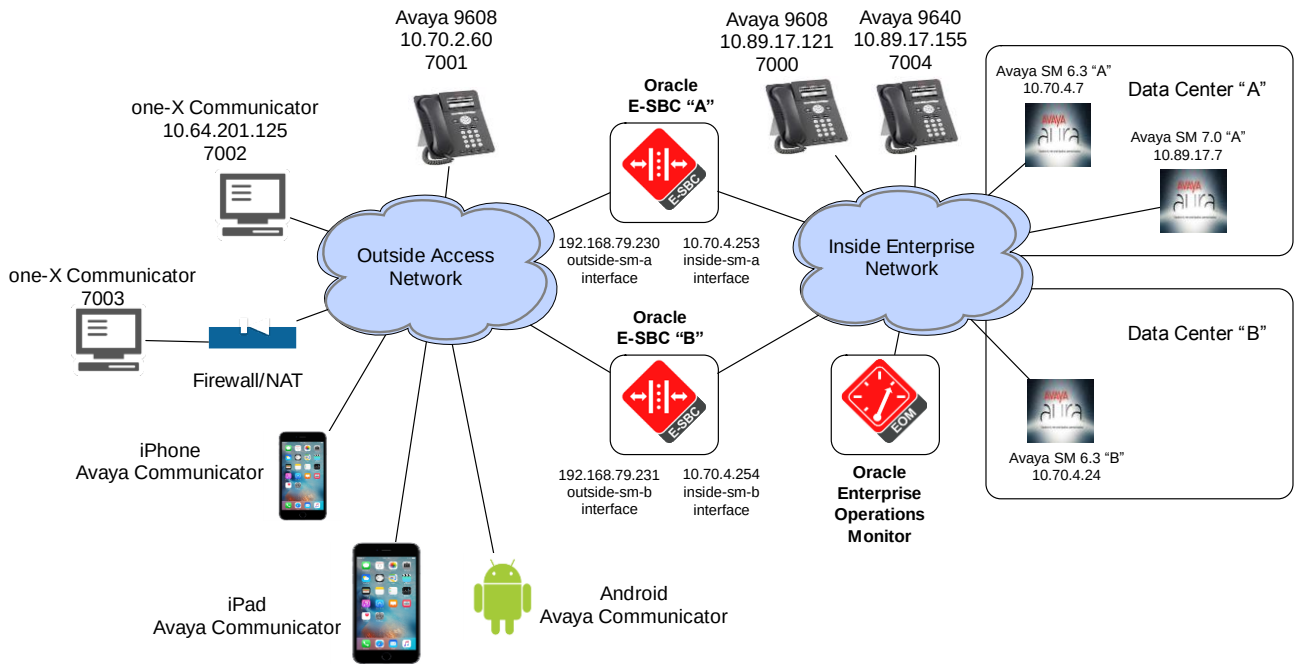
The Oracle Enterprise Session Border Controller (E-SBC) is an enterprise-class signaling component designed to simplify communications networks. It connects disparate IP communications networks while mitigating security threats, curing interoperability problems and ensuring reliability.

Requirements

- Oracle Enterprise Session Border Controllers ECZ7.3.0 MR-1 Patch 1
- Oracle Enterprise Operations Monitor 3.3.90.0.0
- Enterprise firewall to allow phone config file downloads
- Avaya Aura 6.3
    - Avaya Aura System Manger 6.3 SP14
    - Avaya Aura Session Manager 6.3 SP13
    - Avaya Aura Communication Manager 6.3
    - Avaya Modular Messaging 5.2.1
    - Avaya Aura Presence Services 6.3.6.8
    - Avaya Aura Utility Server 6.3 SP13
    - Avaya G430 release 34.5.1
    - One X Communicator 6.2 SP7
    - Avaya Deskphone SIP 6.5
- Avaya Aura 7.0
    - Avaya Aura System Manger 7.0.0.1.4212
    - Avaya Aura Session Manager 7.0.0.1.700102
    - Avaya Aura Communication Manager 7.0.0.2.0.441.22684
    - Avaya Aura Communication Manager Messaging 7.0.0.1.0.441.22477
    - Avaya Aura Presence Services 7.0.0.1.1462
    - Avaya Aura Utility Server 7.0.0.1.0.12
    - Avaya G430 release 36.14.0
    - Avaya Engagement Development Platform 3.1
    - One X Communicator 6.2 SP7/SP11
    - Avaya Deskphone SIP 7.0.0.39

Lab Configuration

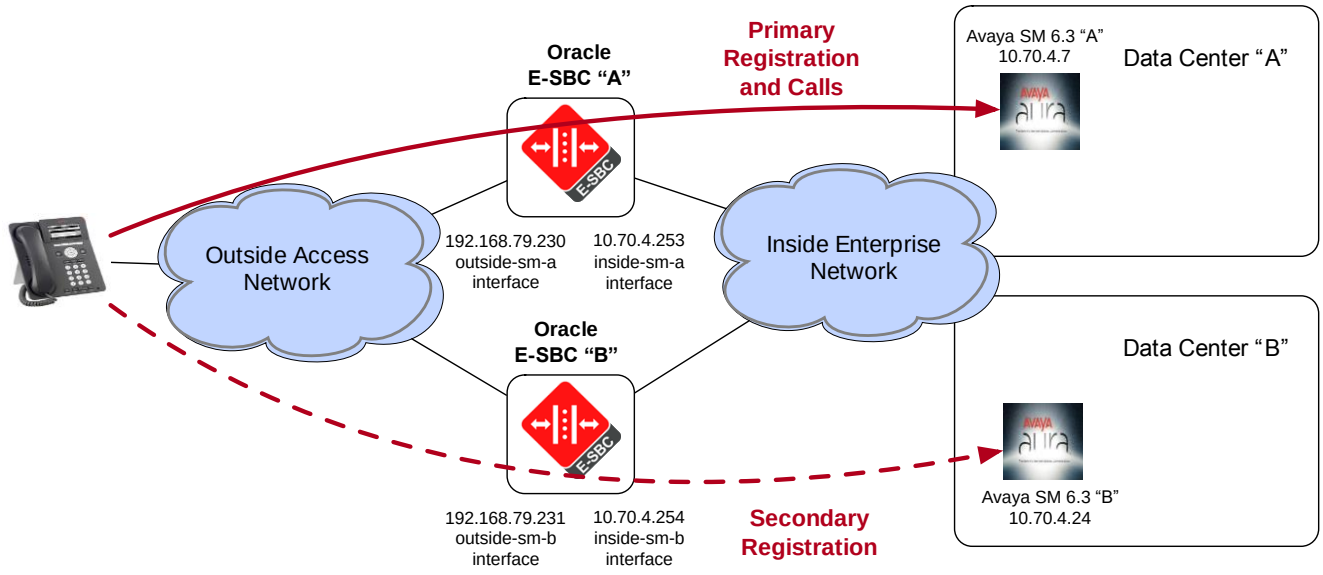
The following diagram illustrates the lab environment created by tekVizion to facilitate certification testing. tekVizion is a systems integrator specifically dedicated to the telecommunications industry. Their core services include consulting/solution design, interoperability/verification testing, integration, custom software development and solution support services.



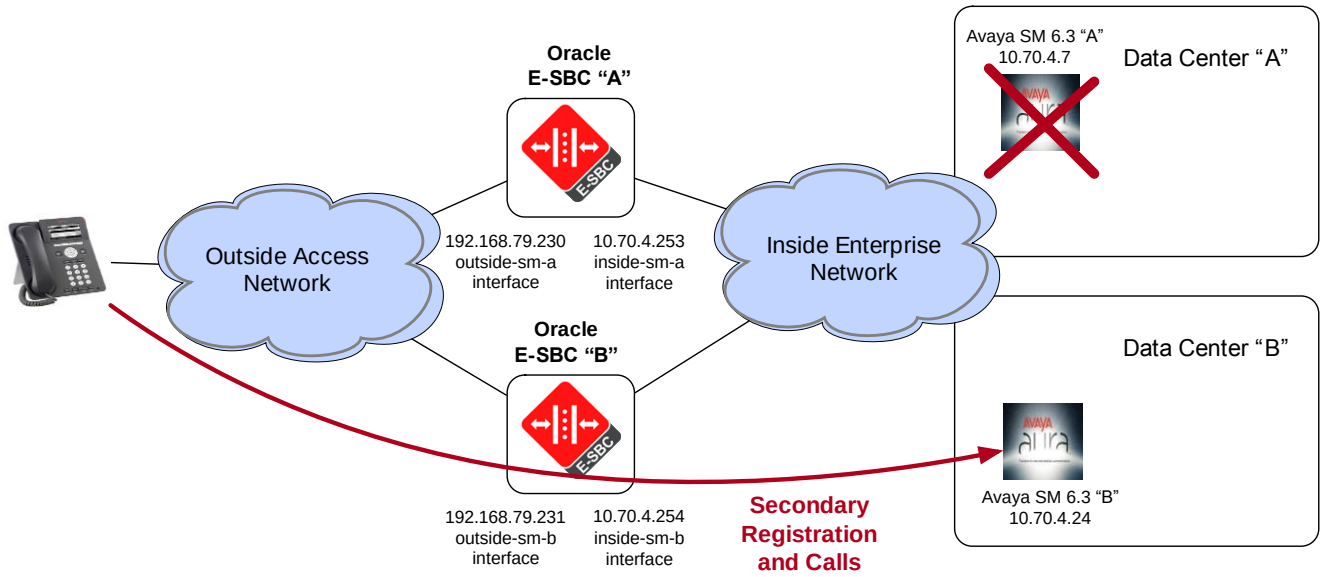
The architecture consists of an "A" site and a "B" site. These can be thought of as separate data centers. The E-SBC "A" can be collocated with Avaya SM "A", and E-SBC B with SM B, but it is not required. There just needs to be IP reachability from the E-SBC A to SM A, and from E-SBC B to SM B. To achieve the highest level of redundancy and high-availability (HA), each SBC should be deployed as an HA pair, so there would be an "A" HA pair, and a "B" HA pair. This can help preserve active calls and establish new calls if one member of the SBC HA pair were to fail, or one of the other components in the call path were to fail, such as a network cable, a router, an Ethernet switch, etc., assuming the other components are also deployed in a redundant fashion. The failover from the "A" data center to the "B" data center would then only occur if the SM A fails or the entire data center goes offline.

The Oracle Enterprise Operations Monitor (EOM) was used to monitor the SIP signaling during testing. The E-SBC was used as a probe to send SIP signaling to EOM for analysis in real time or for historical reporting. Even though the SIP signaling was encrypted using TLS, it can still be read by EOM. The communication between the E-SBC and EOM can be either plaintext or encrypted with TLS.

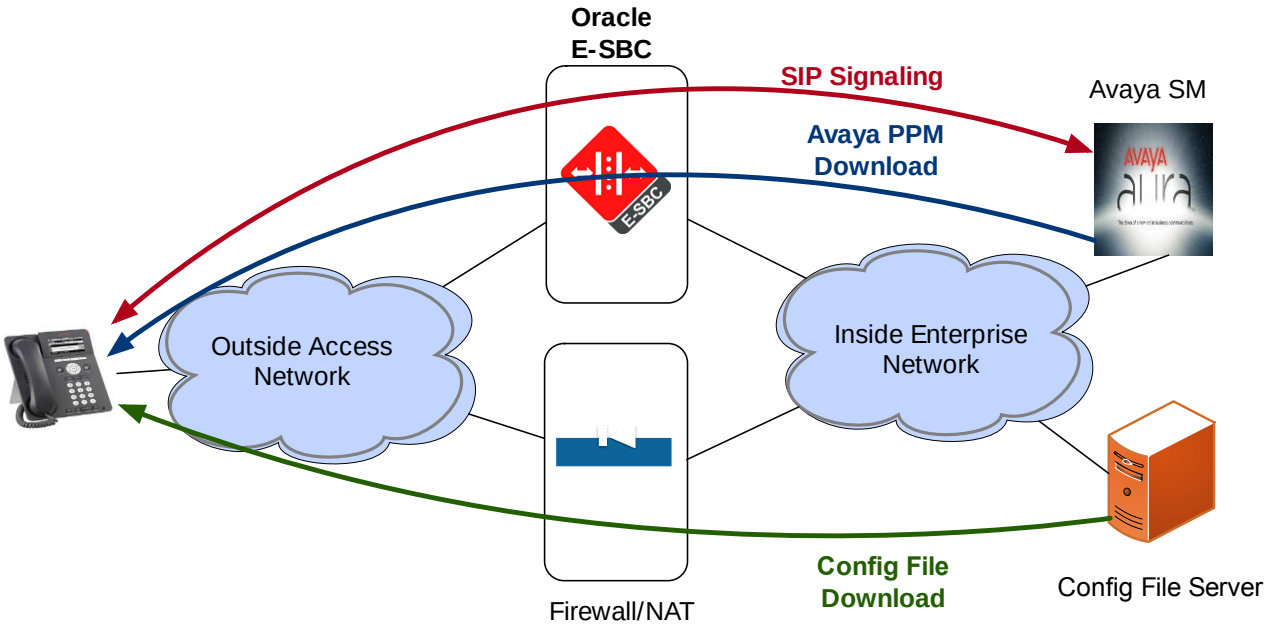
Each phone and soft client is configured to register simultaneously with the A and B Session Managers, as shown in the following diagram.



If the primary SM "A" were to fail, the SBC sends a TCP FIN to all phones/clients, and subsequent registrations to the SBC "A" go unanswered. This causes the phone to failover to the "B" side.



The SIP signaling, Avaya PPM download, and config file downloads take the paths shown in the following diagram.



Caveats

- SM redundancy was only tested with Avaya 6.3 due to lab resource availability, although the same functionality should exist in Avaya 7.0.
- Chat was not tested as the XMPP protocol is not supported through the SBC, although clients may be configured to use chat though the enterprise firewall.
- The Android phone was not tested with Avaya 6.3 because it had an issue logging in even when it was directly connected to the enterprise network, bypassing the SBC.
- Shared Control only works if one user is remote and the other use is local, i.e. both users cannot be remote.

Configuration, validation and troubleshooting is the focus of this document and will be described in four phases:

- Phase 1 – Configuring the Oracle E-SBC
- Phase 2 – Configuring the Oracle EOM
- Phase 3 – Configuring the Avaya Aura Session Manager 6.3
- Phase 4 – Configuring the Avaya Aura Session Manager 7.0

Phase 1 – Configuring the Oracle Enterprise Session Border Controllers

In this section we describe the steps for configuring Oracle Enterprise SBCs (E-SBCs) for use with Avaya Aura Session Manager (SM) 6.3 or 7.0. There is no difference in the E-SBC configuration between 6.3 and 7.0, with the exception of 2048-bit key certificates being supported by Avaya 7.0.

In Scope

The following guide for configuring the Oracle SBC assumes that this is a newly deployed device dedicated to a single customer. Please see the ACLI Configuration Guide on http://docs.oracle.com/cd/E61547_01/index.html for a better understanding of the Command Line Interface (CLI).

Note that Oracle offers several models of the SBC. This document covers the setup for the VME, 1100, 3820, 4500, 4600, and 6300 platforms running OS ECZ7.3.0 MR-1 Patch 1 or later. Each of the products listed above run the same software, configuration and method of implementation. If additional instructions are required, please contact your Oracle sales representative.

Out of Scope

- Configuration of Network management including SNMP and RADIUS
- Configuration of Distributed Denial of Service (DDoS) protection parameters as these are based on individual customer requirements.

What will you need

- RJ45/DB9 serial adapter provided with the SBC, along with a straight-through Ethernet cable to go from the adapter to the SBC's console port (on the rear of the 1100, 4600, and 6300, and the front of the 3820 and 4500).
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle SBC
- IP address to be assigned to the management interface (eth0, labeled Mgmt0 on the SBC chassis) of the SBC - the eth0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support SBC configurations with management and media/service interfaces on the same subnet.
- IP addresses of the Avaya SM and Oracle EOM
- IP addresses to be used for the SBC internal and external facing ports (Service Interfaces)

SBC – Getting Started

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity. **Note: use the console port on the front of the SBC, not the one on the back, on platforms such as the 3820 and 4500 that have two console ports.**

Plug the slot 0 port 0 (s0p0) interface into your outside network and the slot 1 port 0 (s1p0) interface into your inside network. Once connected, you are ready to power on and perform the following steps.

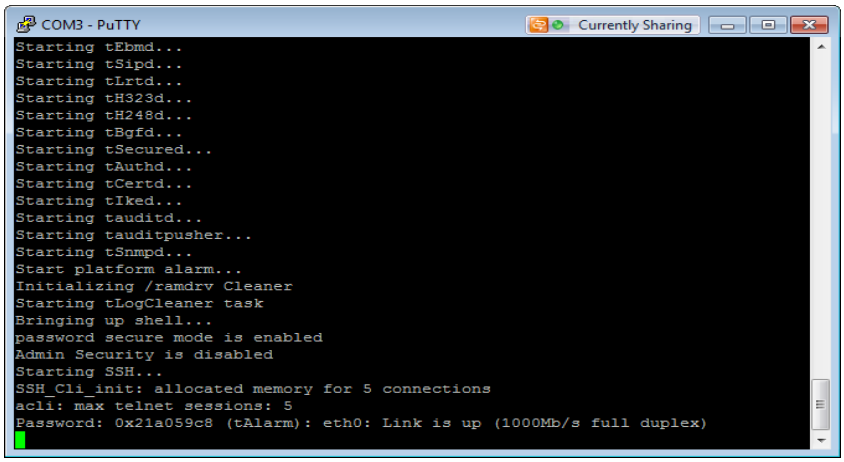
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as **oraclesbc1** are parameters which are specific to an individual deployment. **Note:** The CLI is case sensitive.

Establish the serial connection and logging in the SBC

Confirm the SBC is powered off and connect one end of a straight-through Ethernet cable to the console port on the SBC and the other end to the console adapter that ships with the SBC, connect the console adapter (a DB9 adapter) to the DB9 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 SBC and confirm that you see the following output from the bootup sequence.



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

```
Password: acme
oraclesbc1> enable
Password: packet
oraclesbc1# configure terminal
oraclesbc1(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

oraclesbc1# configure terminal --> bootparam

- Once you type "bootparam" you have to use the "carriage return" key to navigate down
- A reboot is required if changes are made to the existing bootparams. **Note these example boot parameters are specific to the 4600 platform. Other platforms will have different boot parameters. Use nnECZ730m1p1.64.bz software for the 1100, 4500, 4600, and the 6300. Use nnECZ730m1p1.32.bz for the 3820.**

```
    oraclesbc1(configure)# bootparam

    '.' = clear field;   '-' = go to previous field;   q = quit

    Boot File             : /boot/nnECZ730m1p1.64.bz
    IP Address            : 192.168.79.44
    VLAN                  :
```

```
    Netmask                 : 255.255.255.224
    Gateway                 : 192.168.79.33
    IPv6 Address            :
    IPv6 Gateway            :
    Host IP                 : 0.0.0.0
    FTP username            : vxftp
    FTP password            : vxftp123
    Flags                   :
    Target Name             : oraclesbc1
    Console Device          : COM1
    Console Baudrate        : 115200
    Other                   :

    NOTE: These changed parameters will not go into effect until reboot.
    Also, be aware that some boot parameters may also be changed through
    PHY and Network Interface Configurations.
```

Configuring the SBC in the "A" Site/Data Center

The following section walks you through configuring the Oracle Enterprise SBC in the "A" site or data center required to work with Avaya Aura.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

High Availability (Local to a Particular Site)

The Mgmt1 and Mgmt2 (labeled wancom1 and wancom2 in the configuration) ports which are on the rear panel of the SBC are used for the purpose of High Availability on the E-SBC. Crossover cables must be connected between these ports on the SBCs, i.e. Mgmt1 to Mgmt1 and Mgmt2 to Mgmt2. Please refer to the "High Availability Nodes" in the ACLI configuration guide for ECZ730 for more details. Note that HA was not configured in this exercise.

Certificate-Records

Path: **`configure terminal > security > certificate-record`**

```
certificate-record
        name                                    AvayaRootCaCert
        country                                 US
        state                                   TX
        locality                                Plano
        organization                            AVAYA
        unit                                    MGMT
        common-name                             default
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                1024
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        options
certificate-record
        name                                    AvayaSmCaCert
        country                                 US
        state                                   TX
        locality                                Plano
```

```
        organization                            Avaya Inc.
        unit                                    SIP Product Certificate Authority
        common-name                             SIP Product Certificate Authority
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                2048
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        options
certificate-record
        name                                    SbcCertA
        country                                 US
        state                                   TX
        locality                                Plano
        organization                            AVAYA
        unit                                    SDP
        common-name                             tekap1.lab.tekvizion.com
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                1024
NOTE: Avaya 6.3 only supports 1024 bit certificates. Change this to 2048 for Avaya
7.0.
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
                                                clientAuth
NOTE: The command to enter is:
extended-key-usage-list (serverAuth clientAuth)
        options
```

Importing Trusted Certificates

All trusted Certificate Authority (CA) certificates must be imported into the SBC's configuration. This includes the following types of certs:

- All CA(s) that signed the SBC's certificates. This will typically be one CA.
- All CA(s) that signed the SBC's peers' (session-agents') certs, e.g. the CA(s) that signed SM's certificate.

Each trusted certificate must have a certificate-record configured (path: configure terminal > security > certificate-record), followed by a save/activate. The certs can then be imported one at a time using the "import-certificate try-all <certficate-record-name>" command, where the certificate is pasted into the Command Line Interface (CLI) after issuance of the command, followed by a semi-colon (";") to indicate the end of the certificate, and then a save/activate. Here is an example of the certificate importation process after the corresponding certificate-record has been configured and a save/activate has been performed.

oraclesbc1# **import-certificate try-all ExampleCaCert**

IMPORTANT:

Please enter the certificate in the PEM format.

Terminate the certificate with ";" to exit.....

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIBADANBgkqhkiG9w0BAQUFADBvMRUwEwYDVQQDEwwxOTIu
MjAwLjEuMTExEzARBgNVBAsTCkNvbnRyYWN0b3IxDDAKBgNVBAsTA1BLSTEMMAoG
A1UECxMDRG9EMRgwFgYDVQQKEw9VLlMuIEdvdmVybm1lbnQxCzAJBgNVBAYTAlVT
MB4XDTA5MDYwMTIxMzExMloXDTEwMDYwMTIxMzExMlowbzEVMBMGA1UEAxMMMTky
LjIwMC4xLjExMRMwEQYDVQQLEwpDb250cmFjdG9yMQwwCgYDVQQLEwNQS0kxDDAK
BgNVBAsTA0RvRDEYMBYGA1UEChMPVS5TLiBHb3Zlcm5tZW50MQswCQYDVQQGEwJV
UzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygvCYGGWd+zXqo/2waPWBQbU
uLYFD0DCuA+AhemNR/ueiBMnpaBfD6eJwYaVj9jfweTC/EdO3gLuqWsnscgCRKgc
oQcWUBH/EaCFFKlEPnhU8znAr1otr+5I4PvFUZMIeODJ51R4Um2Q3XIRlJrhGNOC
k42juxhYe1Ay2m6qTcECAwEAAaNOMEwwCQYDVR0TBAIwADAgBgNVHSUBAf8EFjAU
BggrBgEFBQcDAQYIKwYBBQUHAwkwHQYDVR0OBBYEFHQy2karD38Xp/Qje2ROAYjI
6SfsMA0GCSqGSIb3DQEBBQUAA4GBAFkNGCLXKl47vA+8p7vbpdmDhC8iZK2dP1b4
5WpflOvQBF/qZg5bj/j8lydU4cXpl9mi9Wt0gxc6DtWZuRfvs5n8Kq8q4juPGjMZ
b/ppsD5++vDe1LlayxlrzQbCZSKkJ8CkixYY4NHk6oAyHMz9OqjVTO1GWS7MZdLp
Sy+Q9Ma3
-----END CERTIFICATE-----**;** ← **Note the semi-colon that was entered after the certificate**

Certificate imported successfully....
WARNING: Configuration changed, run "save-config" command.

oraclesbc1# **save**
checking configuration
Save-Config received, processing.
waiting 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'.
oraclesbc1# **activate-config**
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1#

Generating the SBC's Certificate Signing Requests

The SBC only needs one certificate with the Common Name set to a Fully Qualified Domain Name (FQDN). To generate a certificate signing request, the certificate must be configured as a certificate-record with the appropriate fields (as dictated by the signing CA's policies), followed by a save/activate. Each certificate signing request can then be generated using the "generate-certificate-request <certificate-record-name>". The certificate signing request can then be given to the CA to be signed.
Here is an example generation of a certificate signing request:

generate-certificate-request ExampleSbcCertA

Generating Certificate Signing Request. This can take several minutes....
-----BEGIN CERTIFICATE REQUEST-----

MIIByTCCATICAQAwXjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEXMBUGA1UEAxMOMTky
LjE2OC4xMy4xMTMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANoAWTk8tHzE
tblCL88CFwx9s9soqbKr0u+ZSJQEKsV0OUMtPX60X5+Z94TORp1waZMcSTSHktmR
OrUsF8j9OV/5YvCJFWxvxMXOpivdO9Tbd7M44776P41weIBRXNBv7aWv2qzc4gUx
IFXRcf4xBnyZllLxEwO68ezZxB3y8EUNAgMBAAGgKzApBgNVHQ8xIhMgZGlnaXRh
bFNpZ25hdHVyZSxrZXlFbmNpcGhlcm1lbnQwDQYJKoZIhvcNAQEFBQADgYEAcSZH
6nig6A2GgAnCTUTjraJH/bMHoFQkeXOWcmUf84u6VKyV/9EDhlE/hdjG5/32KIXP
d6zQ7J9GeanvrkSqa757rI2uqbRR/cQlWPNGAG4TocNwdkZznGYm9Du4qPH4ceSh
stD/bBql63NjkSKrQXwpB6VZYfcATH6X++7VRco=
-----END CERTIFICATE REQUEST-----

WARNING: Configuration changed, run "save-config" command.

Then save and activate the configuration; the private key will be stored.
Copy and paste the request, including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" into a text file and give the file to the CA.

Importing the SBC's Signed Certificates

When the signed certificates are received from the CA, they need to be imported into the SBC using the "import-certificate try-all <certificate-record-name>" command as outlined in the "Importing Trusted Certificates" section, followed by a save/activate.

Managing Certificate Expirations to Avoid Service Disruptions

The certificates expire and hence must be properly managed/renewed to avoid service disruptions.

HTTP-ALG

The HTTP-ALG is used for the Avaya Personal Profile Manager (PPM) downloads to the phones/clients. In this example, 10.70.4.7 is the "A" side SM's IP address.

Path: **`configure terminal > session-router > http-alg`**

```
http-alg
        name                                    avaya-sm-a
        state                                   enabled
        description
        http-alg-private
                realm-id                                inside-sm-a
                address                                 10.70.4.253
                destination-address                     10.70.4.7
                destination-port                        443
                tls-profile                             TlsProfile
        http-alg-public
                realm-id                                outside-sm-a
                address                                 192.65.79.230
                port                                    443
                tls-profile                             TlsProfile
        dynamic-acl                             disabled
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
```

Local Policy

Path: **configure terminal > session-router > local-policy**

```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            outside-sm-a
        description
        activate-time
        deactivate-time
        state                                   enabled
        policy-priority                         none
        policy-attribute
                next-hop                                10.70.4.7
                realm                                   inside-sm-a
                action                                  none
                terminate-recursion                     disabled
                carrier
                start-time                              0000
                end-time                                2400
                days-of-week                            U-S
                cost                                    0
                state                                   enabled
                app-protocol
                methods
                media-profiles
                lookup                                  single
                next-key
                eloc-str-lkup                           disabled
                eloc-str-match
```

Media Manager

Path: **configure terminal > media-manager > media-manager > select > done**

```
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
```

Network Interfaces

Path: **`configure terminal > system > network-interface`**

```
network-interface
        name                                    s0p0
        sub-port-id                             0
        description
        hostname
        ip-address                              192.168.79.230
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.128
        gateway                                 192.168.79.129
        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                             192.168.79.230
        ftp-address
        icmp-address                            192.168.79.230
        snmp-address
        telnet-address
        ssh-address
network-interface
```

```
        name                                    s1p0
        sub-port-id                             0
        description
        hostname
        ip-address                              10.70.4.253
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 10.70.4.1
        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                             10.70.4.253
        ftp-address
        icmp-address                            10.70.4.253
        snmp-address
        telnet-address
        ssh-address
```

Physical Interfaces

Path: **configure terminal > system > phy-interface**

```
phy-interface
        name                                    s0p0
        operation-type                          Media
        port                                    0
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
phy-interface
        name                                    s1p0
        operation-type                          Media
        port                                    0
        slot                                    1
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
```

Realm Configs

Path: **configure terminal > media-manager > realm-config**

```
realm-config
        identifier                              inside-sm-a
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s1p0:0
        mm-in-realm                             disabled
        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
        device-id
        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
        spl-options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     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
        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
realm-config
        identifier                              outside-sm-a
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p0:0
        mm-in-realm                             disabled
        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
        device-id
        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
        spl-options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     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
        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
```

Session Agent

Path: **configure terminal > session-router > session-agent**

```
session-agent
        hostname                                10.70.4.7
        ip-address                              10.70.4.7
        port                                    5061
        state                                   enabled
        app-protocol                            SIP
        app-type
        transport-method                        StaticTLS
        realm-id                                inside-sm-a
        egress-realm-id
        description                             Avaya Aura SM A
        carriers
        allow-next-hop-lp                       enabled
        constraints                             disabled
        max-sessions                            0
        max-inbound-sessions                    0
        max-outbound-sessions                   0
        max-burst-rate                          0
        max-inbound-burst-rate                  0
        max-outbound-burst-rate                 0
        max-sustain-rate                        0
        max-inbound-sustain-rate                0
        max-outbound-sustain-rate               0
        min-seizures                            5
        min-asr                                 0
        time-to-resume                          0
        ttr-no-response                         0
        in-service-period                       0
        burst-rate-window                       0
        sustain-rate-window                     0
        req-uri-carrier-mode                    None
        proxy-mode
        redirect-action
        loose-routing                           enabled
        send-media-session                      enabled
        response-map
        ping-method                             OPTIONS;hops=0
        ping-interval                           30
        ping-send-mode                          keep-alive
        ping-all-addresses                      disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query                  hunt
        options
        spl-options
        media-profiles
        in-translationid
        out-translationid
```

```
        trust-me                                disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate               0
        early-media-allow
        invalidate-registrations                disabled
        rfc2833-mode                            none
        rfc2833-payload                         0
        codec-policy
        enforcement-profile
        refer-call-transfer                     disabled
        refer-notify-provisional                none
        reuse-connections                       NONE
        tcp-keepalive                           none
        tcp-reconn-interval                     0
        max-register-burst-rate                 0
        register-burst-window                   0
        sip-profile
        sip-isup-profile
        kpml-interworking                       inherit
        monitoring-filters
        session-recording-server
        session-recording-required              disabled
        hold-refer-reinvite                     disabled
        send-tcp-fin                            enabled
```

SIP Config

Path: **configure terminal > session-router > sip-config > select**

NOTE: Enter each sip option separately with a plus sign in front of it, i.e.
options +global-contact
options +reg-cache-mode=from

```
sip-config
        state                                   enabled
        operation-mode                          dialog
        dialog-transparency                     enabled
        home-realm-id                           inside-sm-a
        egress-realm-id
        auto-realm-id
        nat-mode                                None
        registrar-domain                        *
        registrar-host                          *
        registrar-port                          5060
        register-service-route                  always
        init-timer                              500
        max-timer                               4000
        trans-expire                            32
```

```
        initial-inv-trans-expire                0
        invite-expire                           180
        inactive-dynamic-conn                   32
        enforcement-profile
        pac-method
        pac-interval                            10
        pac-strategy                            PropDist
        pac-load-weight                         1
        pac-session-weight                      1
        pac-route-weight                        1
        pac-callid-lifetime                     600
        pac-user-lifetime                       3600
        red-sip-port                            1988
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        options                                 global-contact
                                                reg-cache-mode=from
        add-reason-header                       disabled
        sip-message-len                         8192
        enum-sag-match                          disabled
        extra-method-stats                      disabled
        extra-enum-stats                        disabled
        rph-feature                             disabled
        nsep-user-sessions-rate                 0
        nsep-sa-sessions-rate                   0
        registration-cache-limit                0
        register-use-to-for-lp                  disabled
        refer-src-routing                       disabled
        add-ucid-header                         disabled
        proxy-sub-events
        allow-pani-for-trusted-only             disabled
        atcf-stn-sr
        atcf-psi-dn
        atcf-route-to-sccas                     disabled
        eatf-stn-sr
        pass-gruu-contact                       disabled
        sag-lookup-on-redirect                  disabled
        set-disconnect-time-on-bye              disabled
        msrp-delayed-bye-timer                  15
        transcoding-realm
        transcoding-agents
        create-dynamic-sa                       disabled
        node-functionality                      P-CSCF
        match-sip-instance                      disabled
        sa-routes-stats                         disabled
        sa-routes-traps                         disabled
        rx-sip-reason-mapping                   disabled
        add-ue-location-in-pani                 disabled
        hold-emergency-calls-for-loc-info       0
```

SIP Feature

Path: **`configure terminal > session-router > sip-feature`**

```
sip-feature
        name                                    eventlist
        realm
        support-mode-inbound                    Pass
        require-mode-inbound                    Pass
        proxy-require-mode-inbound              Pass
        support-mode-outbound                   Pass
        require-mode-outbound                   Pass
        proxy-require-mode-outbound             Pass
```

SIP Interfaces

Path: **configure terminal > session-router > sip-interface**

NOTE: Enter each sip-interface option separately, with a plus sign preceding it, i.e.
options +dropResponse=699
options +reg-via-key
options +reg-via-match

```
sip-interface
        state                                   enabled
        realm-id                                inside-sm-a
        description
        sip-port
                address                                 10.70.4.253
                port                                    5061
                transport-protocol                      TLS
                tls-profile                             TlsProfile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           none
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    disabled
        min-reg-expire                          300
        registration-interval                   3600
        route-to-registrar                      disabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options
        spl-options
        trust-mode                              all
        max-nat-interval                        3600
        nat-int-increment                       10
        nat-test-increment                      30
```

```
        sip-dynamic-hnt                         disabled
        stop-recurse                            401,407
        port-map-start                          0
        port-map-end                            0
        in-manipulationid                       inManipFromInside
        out-manipulationid                      outManipToInside
        sip-ims-feature                         disabled
        sip-atcf-feature                        disabled
        subscribe-reg-event                     disabled
        operator-identifier
        anonymous-priority                      none
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
        inactive-conn-timeout                   0
        untrusted-conn-timeout                  0
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
        term-tgrp-mode                          none
        charging-vector-mode                    pass
        charging-function-address-mode          pass
        ccf-address
        ecf-address
        implicit-service-route                  disabled
        rfc2833-payload                         101
        rfc2833-mode                            transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                       disabled
        sec-agree-pref                          ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        p-early-media-header                    disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                          0
        tunnel-name
        register-keep-alive                     none
        kpml-interworking                       disabled
        msrp-delay-egress-bye                   disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required              disabled
        service-tag
        reg-cache-route                         disabled
sip-interface
```

```
        state                                   enabled
        realm-id                                outside-sm-a
        description
        sip-port
                address                                 192.65.79.230
                port                                    5061
                transport-protocol                      TLS
                tls-profile                             TlsProfile
                allow-anonymous                         registered
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           always
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    enabled
        min-reg-expire                          300
        registration-interval                   120
        route-to-registrar                      enabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options                                 dropResponse=699
                                                reg-via-key
                                                reg-via-match
        spl-options
        trust-mode                              all
        max-nat-interval                        3600
        nat-int-increment                       10
        nat-test-increment                      30
        sip-dynamic-hnt                         disabled
        stop-recurse                            401,407
        port-map-start                          0
        port-map-end                            0
        in-manipulationid
        out-manipulationid                      outManipToOutside
        sip-ims-feature                         disabled
        sip-atcf-feature                        disabled
        subscribe-reg-event                     disabled
        operator-identifier
        anonymous-priority                      none
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
        inactive-conn-timeout                   0
        untrusted-conn-timeout                  0
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
```

```
        term-tgrp-mode                          none
        charging-vector-mode                    pass
        charging-function-address-mode          pass
        ccf-address
        ecf-address
        implicit-service-route                  disabled
        rfc2833-payload                         101
        rfc2833-mode                            transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                       disabled
        sec-agree-pref                          ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        p-early-media-header                    disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                          0
        tunnel-name
        register-keep-alive                     none
        kpml-interworking                       disabled
        msrp-delay-egress-bye                   disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required              disabled
        service-tag
        reg-cache-route                         disabled
```

SIP Manipulations (Header Manipulation Rules – HMR)

Path: **`configure terminal > session-router > sip-manipulation`**

```
sip-manipulation
        name                                    NAT_IP
        description
        split-headers
        join-headers
        header-rule
                name                                    natFrom
                header-name                             From
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
```

```
                new-value
                element-rule
                        name                                    natFromHost
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $LOCAL_IP
        header-rule
                name                                    natTo
                header-name                             To
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    natToHost
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $REMOTE_IP
sip-manipulation
        name                                    inManipFromInside
        description
        split-headers
        join-headers
        header-rule
                name                                    respond200toOptions
                header-name                             To
                action                                  reject
                comparison-type                         case-sensitive
                msg-type                                request
                methods                                 OPTIONS
                match-value
                new-value                               200
        last-modified-by                        admin@73.182.58.50
        last-modified-date                      2016-03-09 10:12:30
sip-manipulation
        name                                    natNotifyXml
        description
        split-headers
        join-headers
        header-rule
                name                                    modXml
                header-name                             Content-Type
                action                                  manipulate
                comparison-type                         pattern-rule
                msg-type                                request
                methods                                 NOTIFY
```

```
                match-value
                new-value
                element-rule
                        name                                    natRegInfoXml
                        parameter-name                          application/reginfo+xml
                        type                                    mime
                        action                                  find-replace-all
                        match-val-type                          ip
                        comparison-type                         pattern-rule
                        match-value                  (\b(?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
NOTE: The question mark must be escaped in the ACLI with a backslash.  Here is the
command to enter:
match-value (\b(\?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
                        new-value                               $LOCAL_IP
                element-rule
                        name                                    natDialogInfoXml
                        parameter-name                        application/dialog-info+xml
                        type                                    mime
                        action                                  find-replace-all
                        match-val-type                          ip
                        comparison-type                         pattern-rule
                        match-value                  (\b(?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
NOTE: The question mark must be escaped in the ACLI with a backslash.  Here is the
command to enter:
match-value (\b(\?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
                        new-value                               $LOCAL_IP
sip-manipulation
        name                                    outManipToInside
        description
        split-headers
        join-headers
        header-rule
                name                                    natIP
                header-name                             To
                action                                  sip-manip
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value                               NAT_IP
sip-manipulation
        name                                    outManipToOutside
        description
        split-headers
        join-headers
        header-rule
                name                                    natIP
                header-name                             To
                action                                  sip-manip
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value                               NAT_IP
        header-rule
                name                                    natNotifyXml
```

```
                header-name                         To
                action                              sip-manip
                comparison-type                     case-sensitive
                msg-type                            request
                methods                             NOTIFY
                match-value
                new-value                           natNotifyXml
        header-rule
NOTE: This header rule changes a 503 reponse to a REGISTER to be 699, which in
conjunction with the dropReponse=699 sip-interface option causes the SBC's response to be
dropped when the Avaya SM is out of service.  This causes the phone to use its secondary
SBC/SM for registrations and calls.
                name                                change503to699
                header-name                         @status-line
                action                              manipulate
                comparison-type                     case-sensitive
                msg-type                            reply
                methods                             REGISTER
                match-value
                new-value
                element-rule
                        name                                changeStatusCode
                        parameter-name
                        type                                status-code
                        action                              replace
                        match-val-type                      any
                        comparison-type                     case-sensitive
                        match-value                         503
                        new-value                           699
```

Steering Pools

Path: **configure terminal > media-manager > steering-pool**

```
steering-pool
        ip-address                              10.70.4.253
        start-port                              49152
        end-port                                65535
        realm-id                                inside-sm-a
        network-interface
steering-pool
        ip-address                              192.65.79.230
        start-port                              49152
        end-port                                65535
        realm-id                                outside-sm-a
        network-interface
```

System Config

Path: **configure terminal > system > system-config > select**

```
system-config
        hostname
        description                             Oracle 4600 SBC for Avaya Line-Side
Testing
        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
        enable-mblk_tracking                    disabled
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        system-log-level                        WARNING
        process-log-level                       DEBUG
NOTE: This should be changed to NOTICE after intial testing for performance reasons
        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
        comm-monitor
```

```
                state                                   enabled
                sbc-grp-id                              0
                tls-profile
                qos-enable                              enabled
                interim-qos-update                      disabled
                monitor-collector
                        address                                 10.64.4.139
NOTE:  This is the IP address of the Oracle Enterprise Operations Monitor (EOM)
                        port                                    4739
                        network-interface                       wancom0:0
        call-trace                              disabled
        internal-trace                          disabled
        log-filter                              all
        default-gateway                         192.168.79.33
        restart                                 enabled
        exceptions
        telnet-timeout                          0
        console-timeout                         0
        remote-control                          enabled
        cli-audit-trail                         enabled
        link-redundancy-state                   disabled
        source-routing                          enabled
        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
```

TLS Profile

Path: **configure terminal > security > tls-profile**

```
tls-profile
        name                                    TlsProfile
        end-entity-certificate                  SbcCertA
        trusted-ca-certificates                 AvayaRootCaCert
                                                AvayaSmCaCert
        cipher-list                             ALL
        verify-depth                            10
        mutual-authenticate                     disabled
        tls-version                             tlsv1
        options
        cert-status-check                       disabled
        cert-status-profile-list
        ignore-dead-responder                   disabled
        allow-self-signed-cert                  disabled
```

Web Server Config

Path: **`configure terminal > system > web-server-config > select`**

```
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        tls-profile
```

Save, Activate, and Reboot

You will now save your configuration with the **`save-config`** command. This will make it persistent through reboots, but it will not take effect until after you issue the **`activate-config`** command. Some config elements are not Real-Time Configuration (RTC) supported, so a reboot is required after the initial configuration.

```
oraclesbc1# save-config
checking configuration
Save-Config received, processing.
waiting 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'.
oraclesbc1# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1# reboot force
```

The E-SBC “A” site configuration is now complete.

Configuring the SBC in the "B" Site/Data Center

The following section walks you through configuring the Oracle Enterprise SBC in the "B" site or data center required to work with Avaya Aura. Most of the configuration is the same as the "A" site, with the exception of certificates, IP addresses, and naming conventions, e.g. inside-sm-b instead of inside-sm-a.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

High Availability (Local to a Particular Site)

The Mgmt1 and Mgmt2 (labeled wancom1 and wancom2 in the configuration) ports which are on the rear panel of the SBC are used for the purpose of High Availability on the E-SBC. Crossover cables must be connected between these ports on the SBCs, i.e. Mgmt1 to Mgmt1 and Mgmt2 to Mgmt2. Please refer to the "High Availability Nodes" in the ACLI configuration guide for ECZ730 for more details. Note that HA was not configured in this exercise.

Certificate-Records

Path: **`configure terminal > security > certificate-record`**

```
certificate-record
        name                                    AvayaRootCaCert
        country                                 US
        state                                   TX
        locality                                Plano
        organization                            AVAYA
        unit                                    MGMT
        common-name                             default
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                1024
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        options
certificate-record
        name                                    AvayaSmCaCert
NOTE: This is different from the certificate in the "A" site since the "B" site SM
was used as the CA for the "B" site.
        country                                 US
        state                                   TX
        locality                                Plano
        organization                            Avaya Inc.
        unit                                    SIP Product Certificate Authority
        common-name                             SIP Product Certificate Authority
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                2048
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
        options
```

```
certificate-record
        name                                    SbcCertB
        country                                 US
        state                                   TX
        locality                                Plano
        organization                            AVAYA
        unit                                    SDP
        common-name                             tekap2.lab.tekvizion.com
        key-algor                               rsa
        digest-algor                            sha1
        key-size                                1024
NOTE: Avaya 6.3 only supports 1024 bit certificates. Change this to 2048 for Avaya
7.0.
        ecdsa-key-size                          p256
        alternate-name
        trusted                                 enabled
        key-usage-list                          digitalSignature
                                                keyEncipherment
        extended-key-usage-list                 serverAuth
                                                clientAuth
NOTE: The command to enter is:
extended-key-usage-list (serverAuth clientAuth)
        options
```

Importing Trusted Certificates

See the "A" site configuration for instructions on importing trusted certificates.

Generating the SBC's Certificate Signing Requests

See the "A" site configuration for instructions on generating Certificate Signing Requests (CSRs).

Importing the SBC's Signed Certificates

See the "A" site configuration for instructions on importing the SBC's signed certificates.

Managing Certificate Expirations to Avoid Service Disruptions

The certificates expire and hence must be properly managed/renewed to avoid service disruptions.

HTTP-ALG

The HTTP-ALG is used for the Avaya Personal Profile Manager (PPM) downloads to the phones/clients. In this example, 10.70.4.24 is the "B" site SM's IP address.

Path: **`configure terminal > session-router > http-alg`**

```
http-alg
        name                                    avaya-sm-b
        state                                   enabled
        description
        http-alg-private
                realm-id                                inside-sm-b
                address                                 10.70.4.254
```

```
                destination-address                     10.70.4.24
                destination-port                        443
                tls-profile                             TlsProfile
        http-alg-public
                realm-id                                outside-sm-b
                address                                 192.65.79.231
                port                                    443
                tls-profile                             TlsProfile
        dynamic-acl                             disabled
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
```

Local Policy

Path: **configure terminal > session-router > local-policy**

```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            outside-sm-b
        description
        activate-time
        deactivate-time
        state                                   enabled
        policy-priority                         none
        policy-attribute
                next-hop                                10.70.4.24
                realm                                   inside-sm-b
                action                                  none
                terminate-recursion                     disabled
                carrier
                start-time                              0000
                end-time                                2400
                days-of-week                            U-S
                cost                                    0
                state                                   enabled
                app-protocol
                methods
                media-profiles
                lookup                                  single
                next-key
                eloc-str-lkup                           disabled
                eloc-str-match
```

Media Manager

Path: **configure terminal > media-manager > media-manager > select > done**

```
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
```

Network Interfaces

Path: **`configure terminal > system > network-interface`**

```
network-interface
        name                                    s0p0
        sub-port-id                             0
        description
        hostname
        ip-address                              192.168.79.231
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.128
        gateway                                 192.168.79.129
        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                             192.168.79.231
        ftp-address
        icmp-address                            192.168.79.231
        snmp-address
        telnet-address
        ssh-address
network-interface
        name                                    s1p0
        sub-port-id                             0
        description
        hostname
        ip-address                              10.70.4.254
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.255.0
        gateway                                 10.70.4.1
        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                             10.70.4.254
        ftp-address
        icmp-address                            10.70.4.254
        snmp-address
        telnet-address
        ssh-address
```

Physical Interfaces

Path: **configure terminal > system > phy-interface**

```
phy-interface
        name                                    s0p0
        operation-type                          Media
        port                                    0
        slot                                    0
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
phy-interface
        name                                    s1p0
        operation-type                          Media
        port                                    0
        slot                                    1
        virtual-mac
        admin-state                             enabled
        auto-negotiation                        enabled
        duplex-mode                             FULL
        speed                                   100
        wancom-health-score                     50
        overload-protection                     disabled
```

Realm Configs

Path: **configure terminal > media-manager > realm-config**

```
realm-config
        identifier                              inside-sm-b
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s1p0:0
        mm-in-realm                             disabled
        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
        device-id
        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
        spl-options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     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
        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
realm-config
        identifier                              outside-sm-b
        description
        addr-prefix                             0.0.0.0
        network-interfaces                      s0p0:0
        mm-in-realm                             disabled
        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
        device-id
        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
        spl-options
        accounting-enable                       enabled
        net-management-control                  disabled
        delay-media-update                      disabled
        refer-call-transfer                     disabled
        hold-refer-reinvite                     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
        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
```

Session Agent

Path: **configure terminal > session-router > session-agent**

```
session-agent
        hostname                                10.70.4.24
        ip-address                              10.70.4.24
        port                                    5061
        state                                   enabled
        app-protocol                            SIP
        app-type
        transport-method                        StaticTLS
        realm-id                                inside-sm-b
        egress-realm-id
        description                             Avaya Aura SM B
        carriers
        allow-next-hop-lp                       enabled
        constraints                             disabled
        max-sessions                            0
        max-inbound-sessions                    0
        max-outbound-sessions                   0
        max-burst-rate                          0
        max-inbound-burst-rate                  0
        max-outbound-burst-rate                 0
        max-sustain-rate                        0
        max-inbound-sustain-rate                0
        max-outbound-sustain-rate               0
        min-seizures                            5
        min-asr                                 0
        time-to-resume                          0
        ttr-no-response                         0
        in-service-period                       0
        burst-rate-window                       0
        sustain-rate-window                     0
        req-uri-carrier-mode                    None
        proxy-mode
        redirect-action
        loose-routing                           enabled
        send-media-session                      enabled
        response-map
        ping-method                             OPTIONS;hops=0
        ping-interval                           30
        ping-send-mode                          keep-alive
        ping-all-addresses                      disabled
        ping-in-service-response-codes
        out-service-response-codes
        load-balance-dns-query                  hunt
        options
        spl-options
        media-profiles
        in-translationid
        out-translationid
```

```
        trust-me                                disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate               0
        early-media-allow
        invalidate-registrations                disabled
        rfc2833-mode                            none
        rfc2833-payload                         0
        codec-policy
        enforcement-profile
        refer-call-transfer                     disabled
        refer-notify-provisional                none
        reuse-connections                       NONE
        tcp-keepalive                           none
        tcp-reconn-interval                     0
        max-register-burst-rate                 0
        register-burst-window                   0
        sip-profile
        sip-isup-profile
        kpml-interworking                       inherit
        monitoring-filters
        session-recording-server
        session-recording-required              disabled
        hold-refer-reinvite                     disabled
        send-tcp-fin                            enabled
```

SIP Config

Path: **configure terminal > session-router > sip-config > select**

```
sip-config
        state                                   enabled
        operation-mode                          dialog
        dialog-transparency                     enabled
        home-realm-id                           inside-sm-b
        egress-realm-id
        auto-realm-id
        nat-mode                                None
        registrar-domain                        *
        registrar-host                          *
        registrar-port                          5060
        register-service-route                  always
        init-timer                              500
        max-timer                               4000
        trans-expire                            32
        initial-inv-trans-expire                0
```

```
        invite-expire                           180
        inactive-dynamic-conn                   32
        enforcement-profile
        pac-method
        pac-interval                            10
        pac-strategy                            PropDist
        pac-load-weight                         1
        pac-session-weight                      1
        pac-route-weight                        1
        pac-callid-lifetime                     600
        pac-user-lifetime                       3600
        red-sip-port                            1988
        red-max-trans                           10000
        red-sync-start-time                     5000
        red-sync-comp-time                      1000
        options                                 global-contact
                                                reg-cache-mode=from
NOTE: Enter each option separately with a plus sign in front of it, i.e.
options +global-contact
options +reg-cache-mode=from
        add-reason-header                       disabled
        sip-message-len                         8192
        enum-sag-match                          disabled
        extra-method-stats                      disabled
        extra-enum-stats                        disabled
        rph-feature                             disabled
        nsep-user-sessions-rate                 0
        nsep-sa-sessions-rate                   0
        registration-cache-limit                0
        register-use-to-for-lp                  disabled
        refer-src-routing                       disabled
        add-ucid-header                         disabled
        proxy-sub-events
        allow-pani-for-trusted-only             disabled
        atcf-stn-sr
        atcf-psi-dn
        atcf-route-to-sccas                     disabled
        eatf-stn-sr
        pass-gruu-contact                       disabled
        sag-lookup-on-redirect                  disabled
        set-disconnect-time-on-bye              disabled
        msrp-delayed-bye-timer                  15
        transcoding-realm
        transcoding-agents
        create-dynamic-sa                       disabled
        node-functionality                      P-CSCF
        match-sip-instance                      disabled
        sa-routes-stats                         disabled
        sa-routes-traps                         disabled
        rx-sip-reason-mapping                   disabled
        add-ue-location-in-pani                 disabled
        hold-emergency-calls-for-loc-info       0
```

SIP Feature

Path: **configure terminal > session-router > sip-feature**

```
sip-feature
        name                                    eventlist
        realm
        support-mode-inbound                    Pass
        require-mode-inbound                    Pass
        proxy-require-mode-inbound              Pass
        support-mode-outbound                   Pass
        require-mode-outbound                   Pass
        proxy-require-mode-outbound             Pass
```

SIP Interfaces

Path: **configure terminal > session-router > sip-interface**

```
sip-interface
        state                                   enabled
        realm-id                                inside-sm-b
        description
        sip-port
                address                                 10.70.4.254
                port                                    5061
                transport-protocol                      TLS
                tls-profile                             TlsProfile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           none
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    disabled
        min-reg-expire                          300
        registration-interval                   3600
        route-to-registrar                      disabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options
        spl-options
        trust-mode                              all
        max-nat-interval                        3600
        nat-int-increment                       10
        nat-test-increment                      30
```

```
        sip-dynamic-hnt                         disabled
        stop-recurse                            401,407
        port-map-start                          0
        port-map-end                            0
        in-manipulationid                       inManipFromInside
        out-manipulationid                      outManipToInside
        sip-ims-feature                         disabled
        sip-atcf-feature                        disabled
        subscribe-reg-event                     disabled
        operator-identifier
        anonymous-priority                      none
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
        inactive-conn-timeout                   0
        untrusted-conn-timeout                  0
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
        term-tgrp-mode                          none
        charging-vector-mode                    pass
        charging-function-address-mode          pass
        ccf-address
        ecf-address
        implicit-service-route                  disabled
        rfc2833-payload                         101
        rfc2833-mode                            transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                       disabled
        sec-agree-pref                          ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        p-early-media-header                    disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                          0
        tunnel-name
        register-keep-alive                     none
        kpml-interworking                       disabled
        msrp-delay-egress-bye                   disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required              disabled
        service-tag
        reg-cache-route                         disabled
sip-interface
```

```
        state                                   enabled
        realm-id                                outside-sm-b
        description
        sip-port
                address                                 192.65.79.231
                port                                    5061
                transport-protocol                      TLS
                tls-profile                             TlsProfile
                allow-anonymous                         registered
                multi-home-addrs
                ims-aka-profile
        carriers
        trans-expire                            0
        initial-inv-trans-expire                0
        invite-expire                           0
        max-redirect-contacts                   0
        proxy-mode
        redirect-action
        contact-mode                            none
        nat-traversal                           always
        nat-interval                            30
        tcp-nat-interval                        90
        registration-caching                    enabled
        min-reg-expire                          300
        registration-interval                   120
        route-to-registrar                      enabled
        secured-network                         disabled
        teluri-scheme                           disabled
        uri-fqdn-domain
        options                                 dropResponse=699
                                                reg-via-key
                                                reg-via-match
NOTE: Enter each option separately, with a plus sign preceding it, i.e.
options +dropResponse=699
options +reg-via-key
options +reg-via-match
        spl-options
        trust-mode                              all
        max-nat-interval                        3600
        nat-int-increment                       10
        nat-test-increment                      30
        sip-dynamic-hnt                         disabled
        stop-recurse                            401,407
        port-map-start                          0
        port-map-end                            0
        in-manipulationid
        out-manipulationid                      outManipToOutside
        sip-ims-feature                         disabled
        sip-atcf-feature                        disabled
        subscribe-reg-event                     disabled
        operator-identifier
        anonymous-priority                      none
        max-incoming-conns                      0
        per-src-ip-max-incoming-conns           0
        inactive-conn-timeout                   0
        untrusted-conn-timeout                  0
```

```
        network-id
        ext-policy-server
        ldap-policy-server
        default-location-string
        term-tgrp-mode                          none
        charging-vector-mode                    pass
        charging-function-address-mode          pass
        ccf-address
        ecf-address
        implicit-service-route                  disabled
        rfc2833-payload                         101
        rfc2833-mode                            transparent
        constraint-name
        response-map
        local-response-map
        sec-agree-feature                       disabled
        sec-agree-pref                          ipsec3gpp
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        p-early-media-header                    disabled
        p-early-media-direction
        add-sdp-profiles
        manipulation-string
        manipulation-pattern
        sip-profile
        sip-isup-profile
        tcp-conn-dereg                          0
        tunnel-name
        register-keep-alive                     none
        kpml-interworking                       disabled
        msrp-delay-egress-bye                   disabled
        send-380-response
        pcscf-restoration
        session-timer-profile
        session-recording-server
        session-recording-required              disabled
        service-tag
        reg-cache-route                         disabled
```

SIP Manipulations (Header Manipulation Rules – HMR)

Path: **`configure terminal > session-router > sip-manipulation`**

```
sip-manipulation
        name                                    NAT_IP
        description
        split-headers
        join-headers
        header-rule
                name                                    natFrom
                header-name                             From
                action                                  manipulate
```

```
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    natFromHost
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $LOCAL_IP
        header-rule
                name                                    natTo
                header-name                             To
                action                                  manipulate
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value
                element-rule
                        name                                    natToHost
                        parameter-name
                        type                                    uri-host
                        action                                  replace
                        match-val-type                          ip
                        comparison-type                         case-sensitive
                        match-value
                        new-value                               $REMOTE_IP
sip-manipulation
        name                                    inManipFromInside
        description
        split-headers
        join-headers
        header-rule
                name                                    respond200toOptions
                header-name                             To
                action                                  reject
                comparison-type                         case-sensitive
                msg-type                                request
                methods                                 OPTIONS
                match-value
                new-value                               200
        last-modified-by                        admin@73.182.58.50
        last-modified-date                      2016-03-09 10:12:30
sip-manipulation
        name                                    natNotifyXml
        description
        split-headers
        join-headers
        header-rule
                name                                    modXml
                header-name                             Content-Type
```

```
                action                                  manipulate
                comparison-type                         pattern-rule
                msg-type                                request
                methods                                 NOTIFY
                match-value
                new-value
                element-rule
                        name                                    natRegInfoXml
                        parameter-name                          application/reginfo+xml
                        type                                    mime
                        action                                  find-replace-all
                        match-val-type                          ip
                        comparison-type                         pattern-rule
                        match-value                     (\b(?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
NOTE: The question mark must be escaped in the ACLI with a backslash.  Here is the
command to enter:
match-value (\b(\?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
                        new-value                               $LOCAL_IP
                element-rule
                        name                                    natDialogInfoXml
                        parameter-name                        application/dialog-info+xml
                        type                                    mime
                        action                                  find-replace-all
                        match-val-type                          ip
                        comparison-type                         pattern-rule
                        match-value                     (\b(?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
NOTE: The question mark must be escaped in the ACLI with a backslash.  Here is the
command to enter:
match-value (\b(\?:\d{1,3}\.){3}\d{1,3}\b)[[:1:]]
                        new-value                               $LOCAL_IP
sip-manipulation
        name                                    outManipToInside
        description
        split-headers
        join-headers
        header-rule
                name                                    natIP
                header-name                             To
                action                                  sip-manip
                comparison-type                         case-sensitive
                msg-type                                request
                methods
                match-value
                new-value                               NAT_IP
sip-manipulation
        name                                    outManipToOutside
        description
        split-headers
        join-headers
        header-rule
                name                                    natIP
                header-name                             To
                action                                  sip-manip
                comparison-type                         case-sensitive
                msg-type                                request
                methods
```

```
                match-value
                new-value                                NAT_IP
        header-rule
                name                                     natNotifyXml
                header-name                              To
                action                                   sip-manip
                comparison-type                          case-sensitive
                msg-type                                 request
                methods                                  NOTIFY
                match-value
                new-value                                natNotifyXml
        header-rule
NOTE: This header rule changes a 503 reponse to a REGISTER to be 699, which in
conjunction with the dropReponse=699 sip-interface option causes the SBC's response to be
dropped when the Avaya SM is out of service.  This causes the phone to use the other
SBC/SM for registrations and calls.
                name                                     change503to699
                header-name                              @status-line
                action                                   manipulate
                comparison-type                          case-sensitive
                msg-type                                 reply
                methods                                  REGISTER
                match-value
                new-value
                element-rule
                        name                                     changeStatusCode
                        parameter-name
                        type                                     status-code
                        action                                   replace
                        match-val-type                           any
                        comparison-type                          case-sensitive
                        match-value                              503
                        new-value                                699
```

Steering Pools

Path: **configure terminal > media-manager > steering-pool**

```
steering-pool
        ip-address                              10.70.4.254
        start-port                              49152
        end-port                                65535
        realm-id                                inside-sm-b
        network-interface
steering-pool
        ip-address                              192.65.79.231
        start-port                              49152
        end-port                                65535
        realm-id                                outside-sm-b
        network-interface
```

System Config

Path: **configure terminal > system > system-config > select**

```
system-config
        hostname
        description                             Oracle 4600 SBC for Avaya Line-Side
Testing
        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
        enable-mblk_tracking                    disabled
        snmp-syslog-his-table-length            1
        snmp-syslog-level                       WARNING
        system-log-level                        WARNING
        process-log-level                       DEBUG
NOTE: This should be changed to NOTICE after intial testing for performance reasons
        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
        comm-monitor
                state                                   enabled
                sbc-grp-id                              0
                tls-profile
                qos-enable                              enabled
                interim-qos-update                      disabled
                monitor-collector
                        address                                 10.64.4.139
NOTE:  This is the IP address of the Oracle Enterprise Operations Monitor (EOM).
                        port                                    4739
                        network-interface                       wancom0:0
        call-trace                              disabled
        internal-trace                          disabled
        log-filter                              all
        default-gateway                         192.168.79.33
        restart                                 enabled
        exceptions
        telnet-timeout                          0
        console-timeout                         0
        remote-control                          enabled
```

```
        cli-audit-trail                         enabled
        link-redundancy-state                   disabled
        source-routing                          enabled
        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
```

TLS Profile

Path: **configure terminal > security > tls-profile**

```
tls-profile
        name                                    TlsProfile
        end-entity-certificate                  SbcCertB
        trusted-ca-certificates                 AvayaRootCaCert
                                                AvayaSmCaCert
        cipher-list                             ALL
        verify-depth                            10
        mutual-authenticate                     disabled
        tls-version                             tlsv1
        options
        cert-status-check                       disabled
        cert-status-profile-list
        ignore-dead-responder                   disabled
        allow-self-signed-cert                  disabled
```

Web Server Config

Path: **configure terminal > system > web-server-config > select**

```
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        tls-profile
```

Save, Activate, and Reboot

You will now save your configuration with the **save-config** command. This will make it persistent through reboots, but it will not take effect until after you issue the **activate-config** command. Some config elements are not Real-Time Configuration (RTC) supported, so a reboot is required after the initial configuration.

```
oraclesbc2# save-config
checking configuration
Save-Config received, processing.
waiting 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'.
oraclesbc2# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc2# reboot force
```

The E-SBC “B” site configuration is now complete.

Phase 2 – Configuring the Oracle Enterprise Operations Monitor

In this section we describe the steps for configuring Oracle Enterprise Operations Monitor (EOM) for use with the Oracle Enterprise SBCs to monitor SIP signaling traffic on the network.

In Scope

The following guide for configuring the Oracle EOM assumes that this is a newly deployed device dedicated to a single customer. Please see the Oracle Communications Session Monitor Installation Guide on http://docs.oracle.com/cd/E60864_01/index.htm for a better understanding of the basic installation.

Out of Scope

- Basic installation as this is covered in Chapters 2 and 3 of the Oracle Communications Session Monitor Installation Guide.
- High availability.

What will you need

- Console access to the EOM server or virtual machine (VM).
- Browser-based HTTPS access to the EOM server after the initial configuration is complete.
- Administrator password for the EOM to be used.
- IP address to be assigned to EOM.

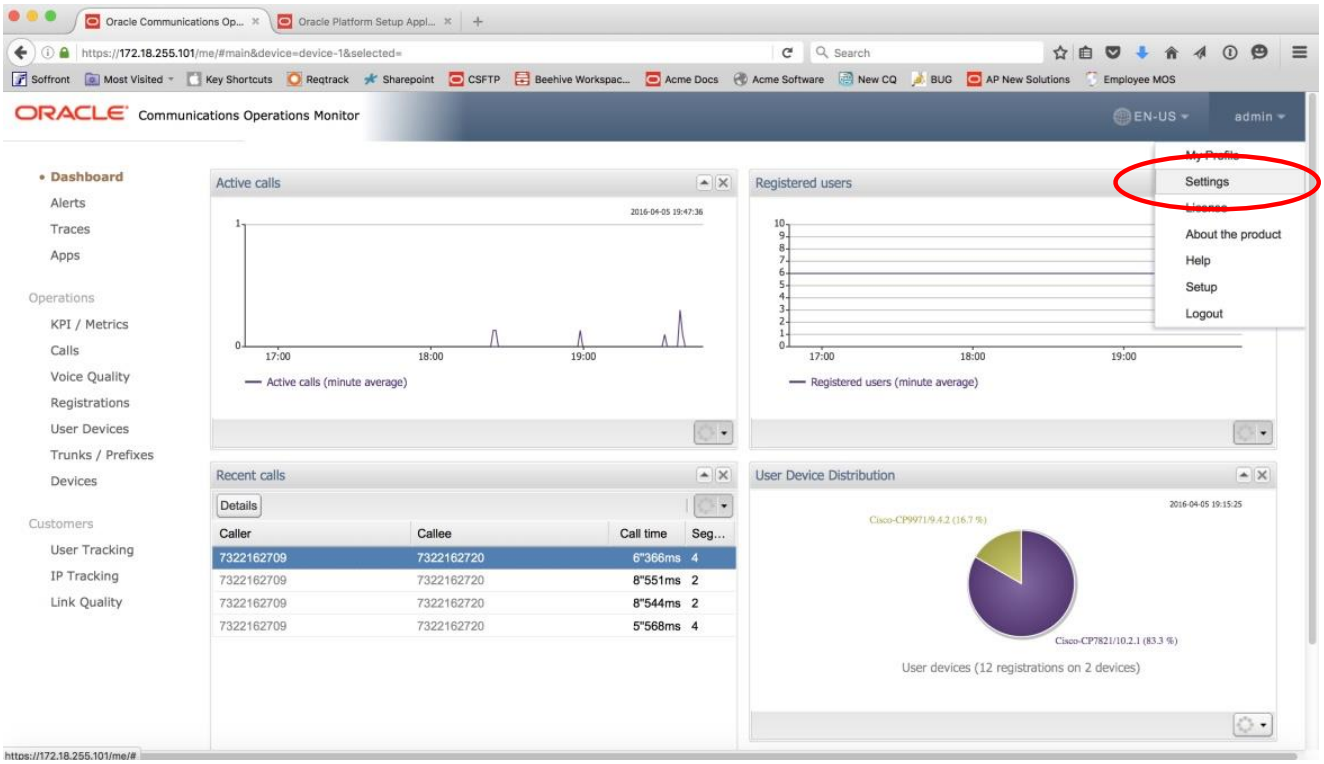
EOM – Getting Started

Ensure that the server or VM specifications meet those outlined in Chapter 1 of the Oracle Communications Session Monitor Installation Guide. Install the EOM software and configure the network parameters as outlined in Chapter 2 of the same guide. Chapter 3 details the subsequent browser-based installation. When prompted to select the “Machine Type”, select the “Communications Operations Monitor” checkbox.

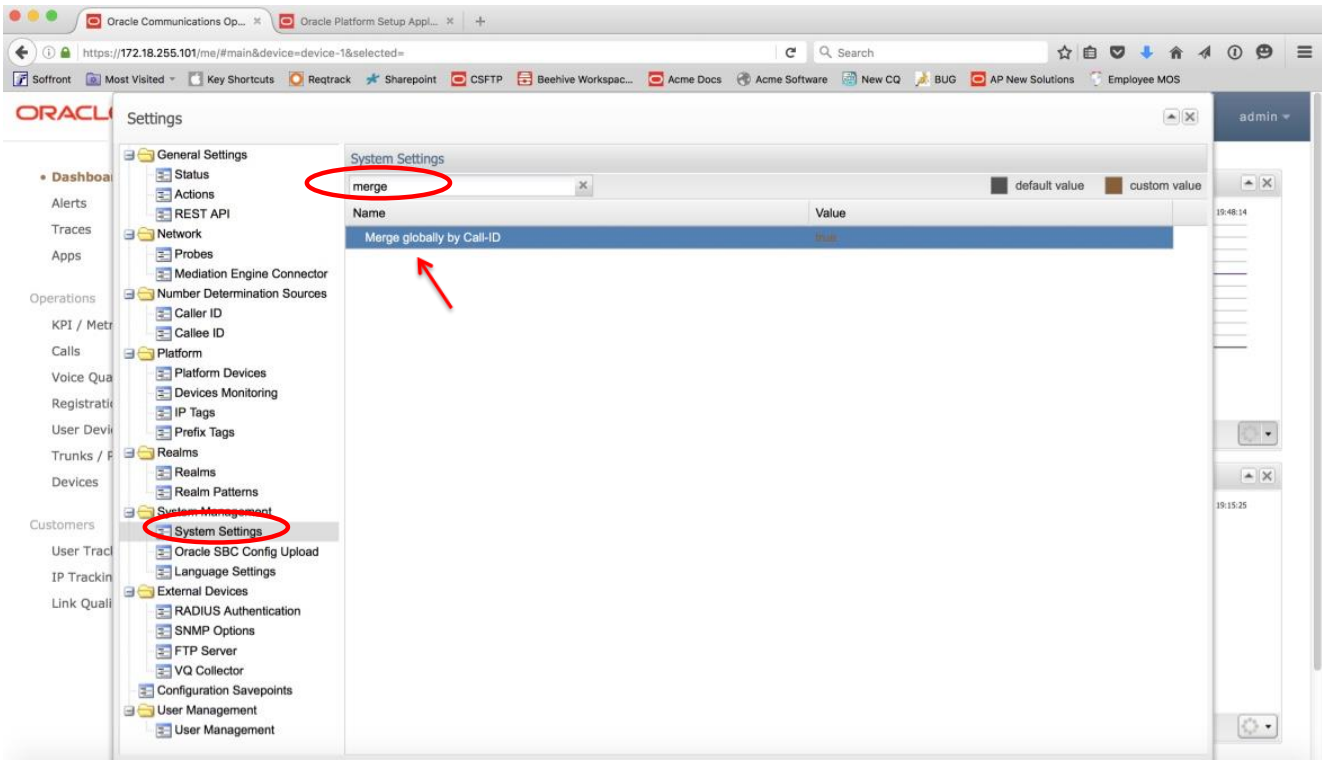
Configuring EOM to Display All Legs of a Call in a Single Report

This allows all call legs on both sides of the E-SBC to be displayed in a single report, making analysis and troubleshooting easier.

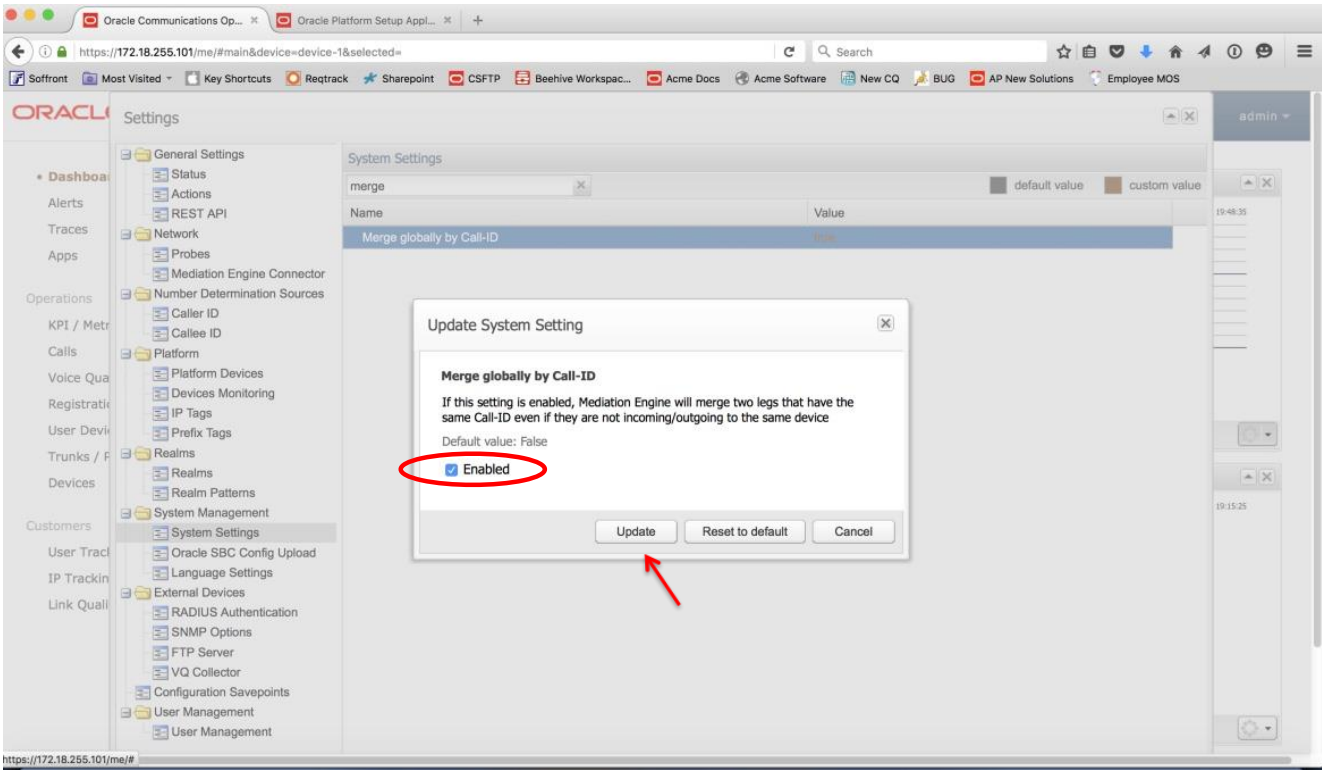
1. Click on the user (admin in this example) in the top right corner, then click on Settings.



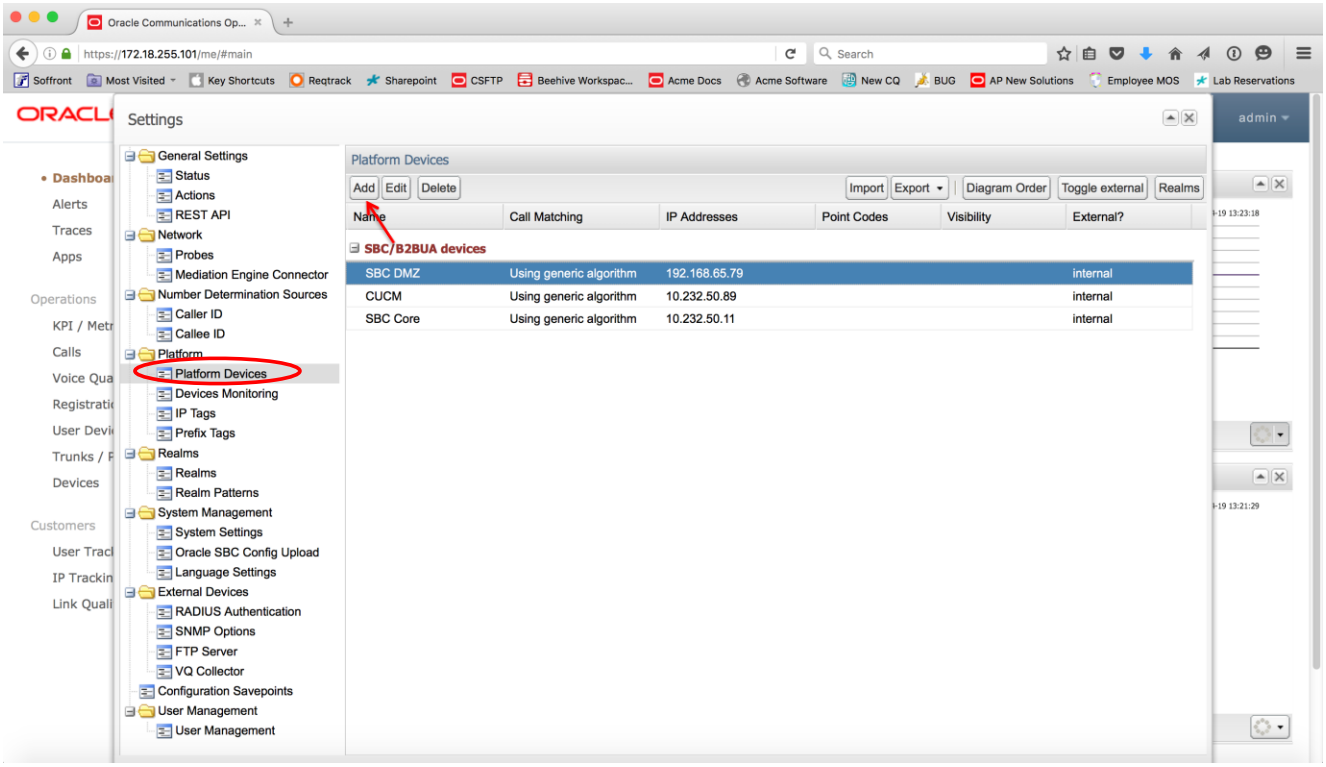
2. Under System Management select System Settings and search for “merge”. Double click on “Merge globally by Call-ID”.



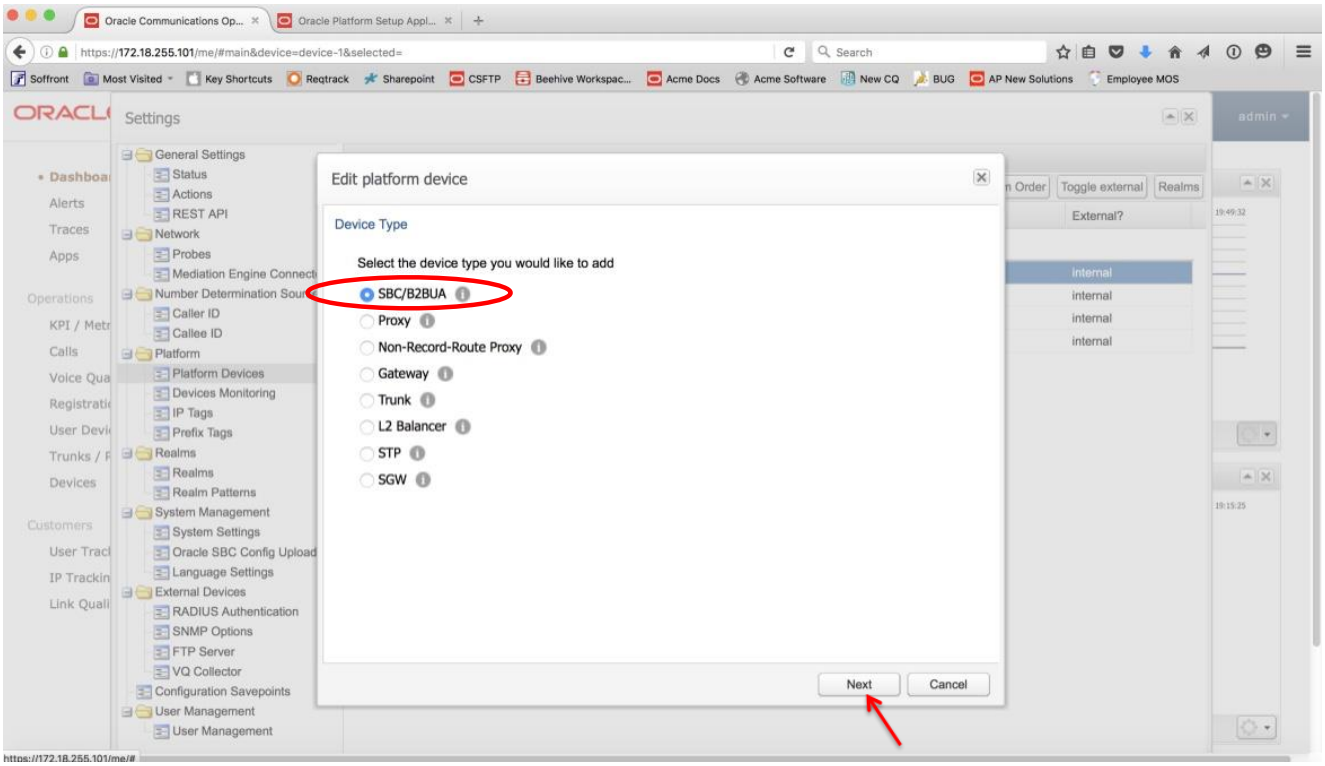
3. Click on the Enabled check box and click Update.



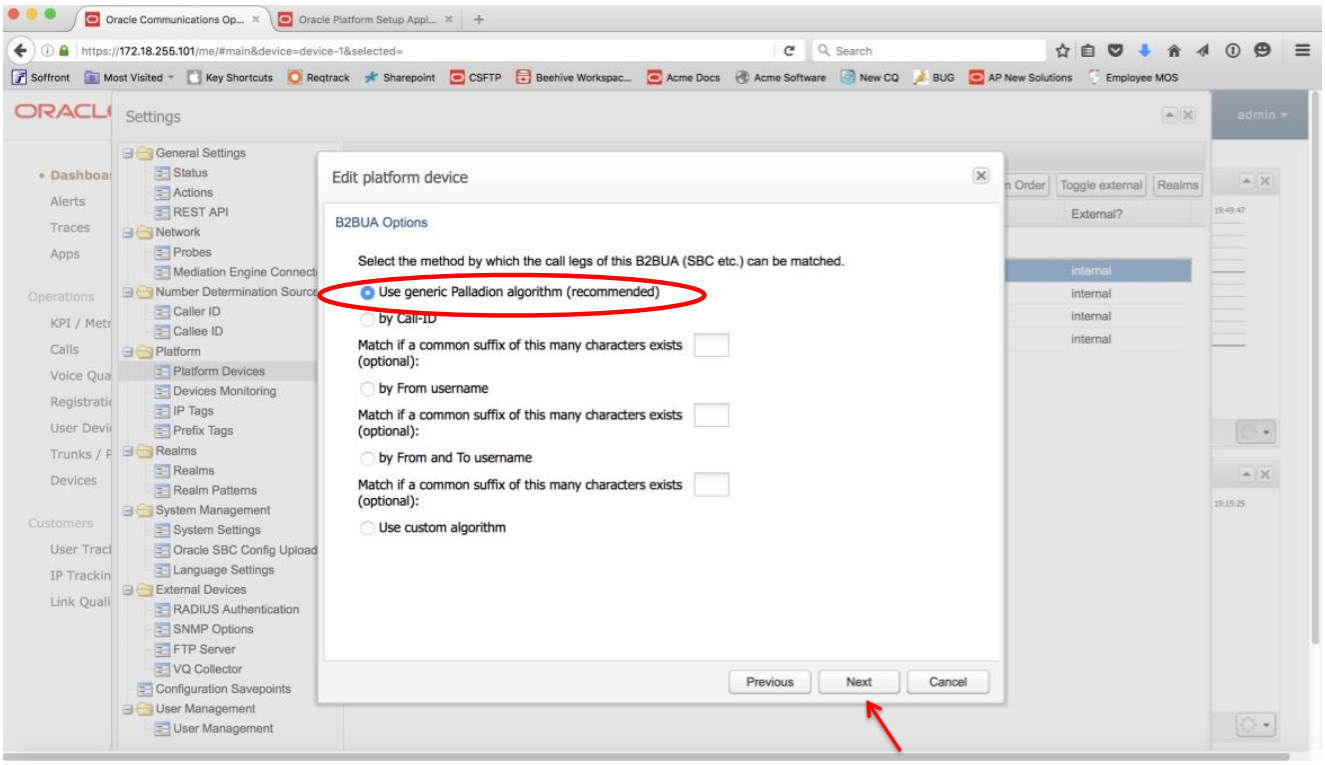
4. Under Platform select Platform Devices. Click Add (or Edit if you've already added a device).



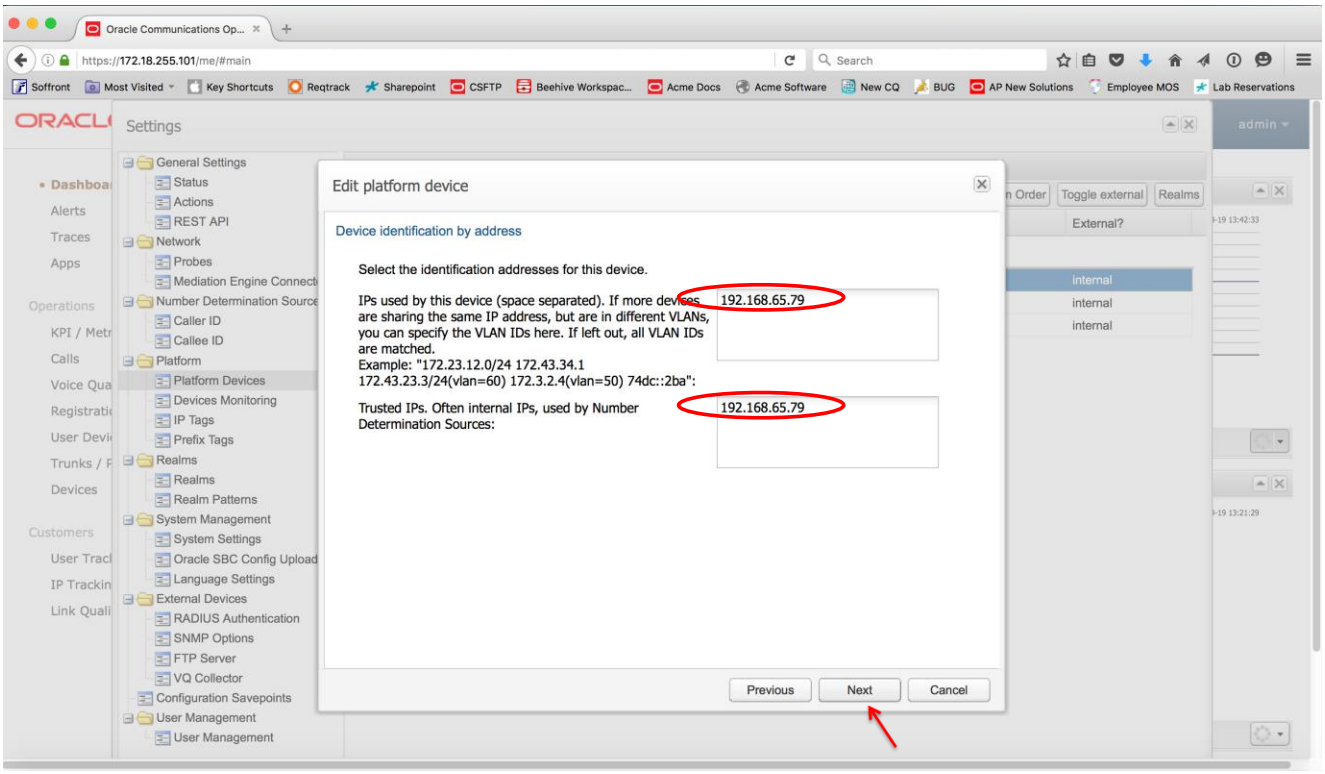
5. Select the SBC/B2BUA radio button regardless of the type of device you're adding, then click Next.



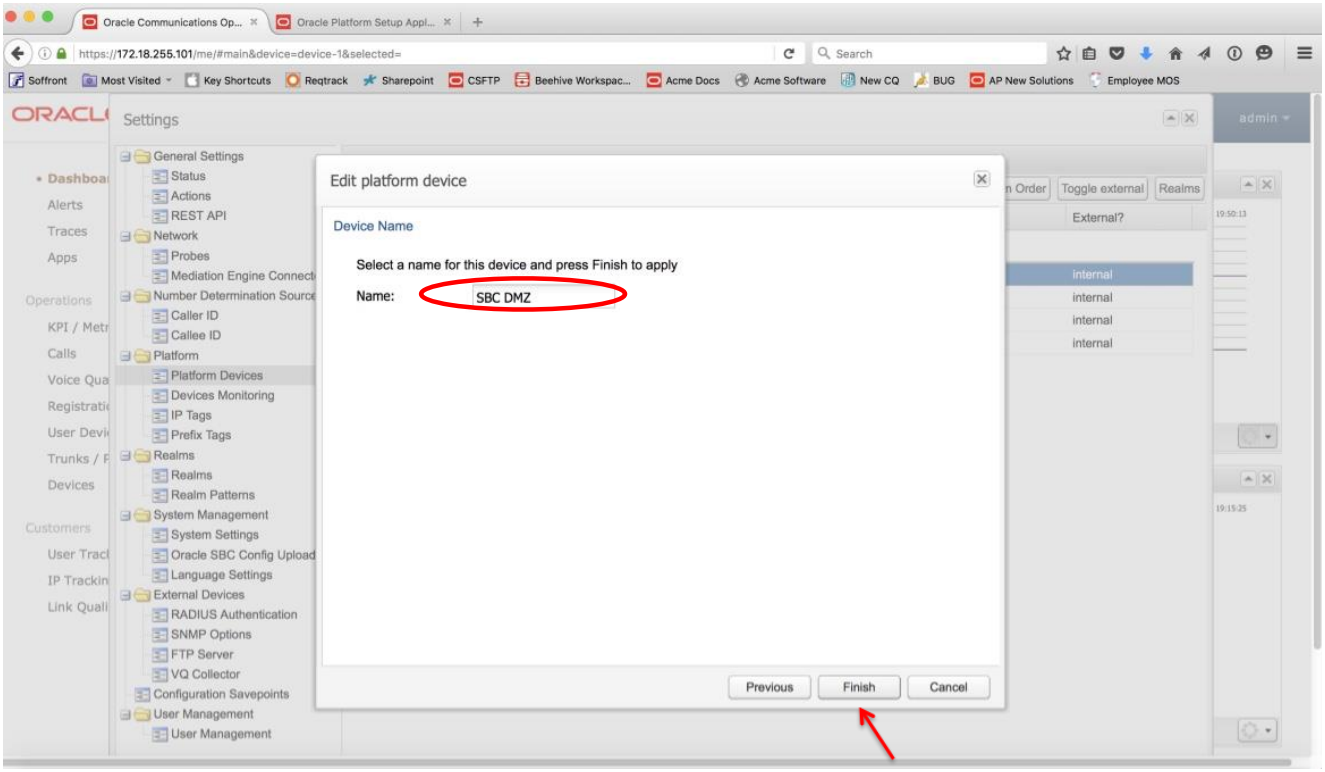
6. Click on the “Use generic Palladion algorithm (recommended)” radio button, then click Next.



7. Enter the device’s IP address in both fields, then click Next.

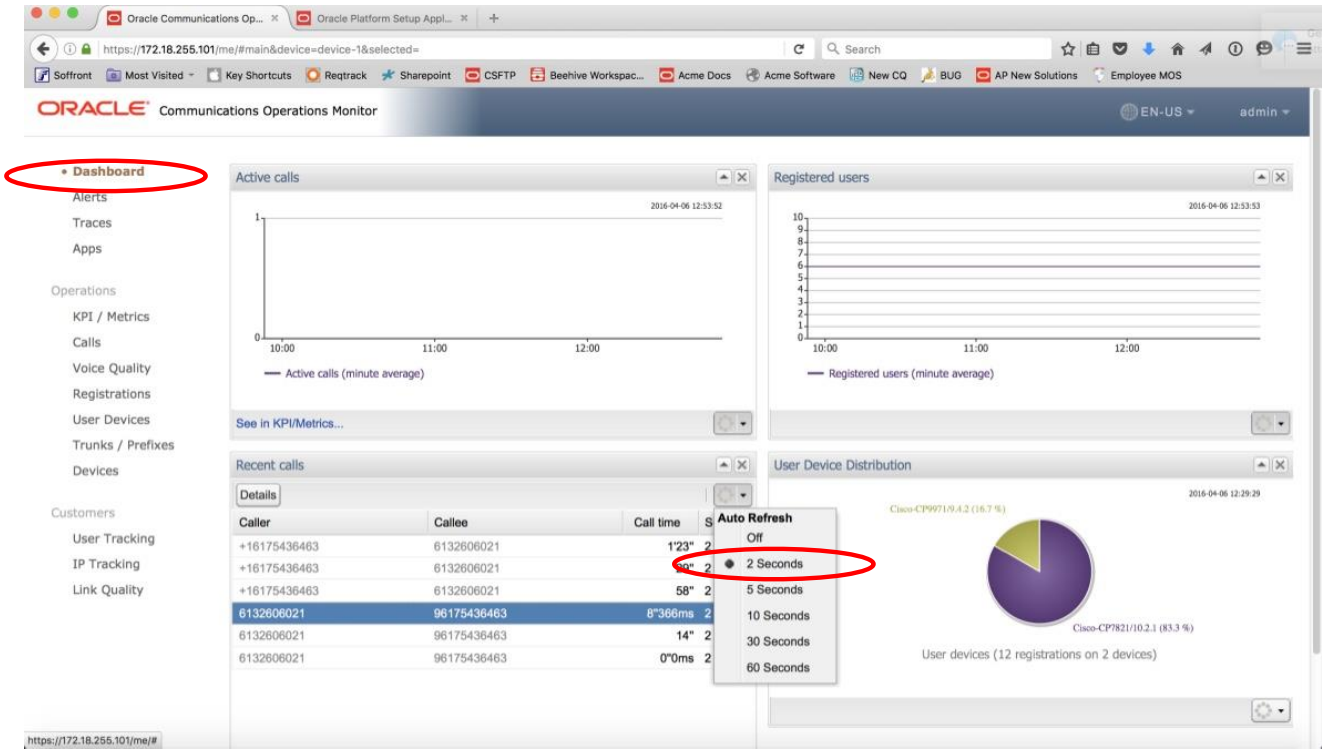


8. Enter a name for the device and click Finish.

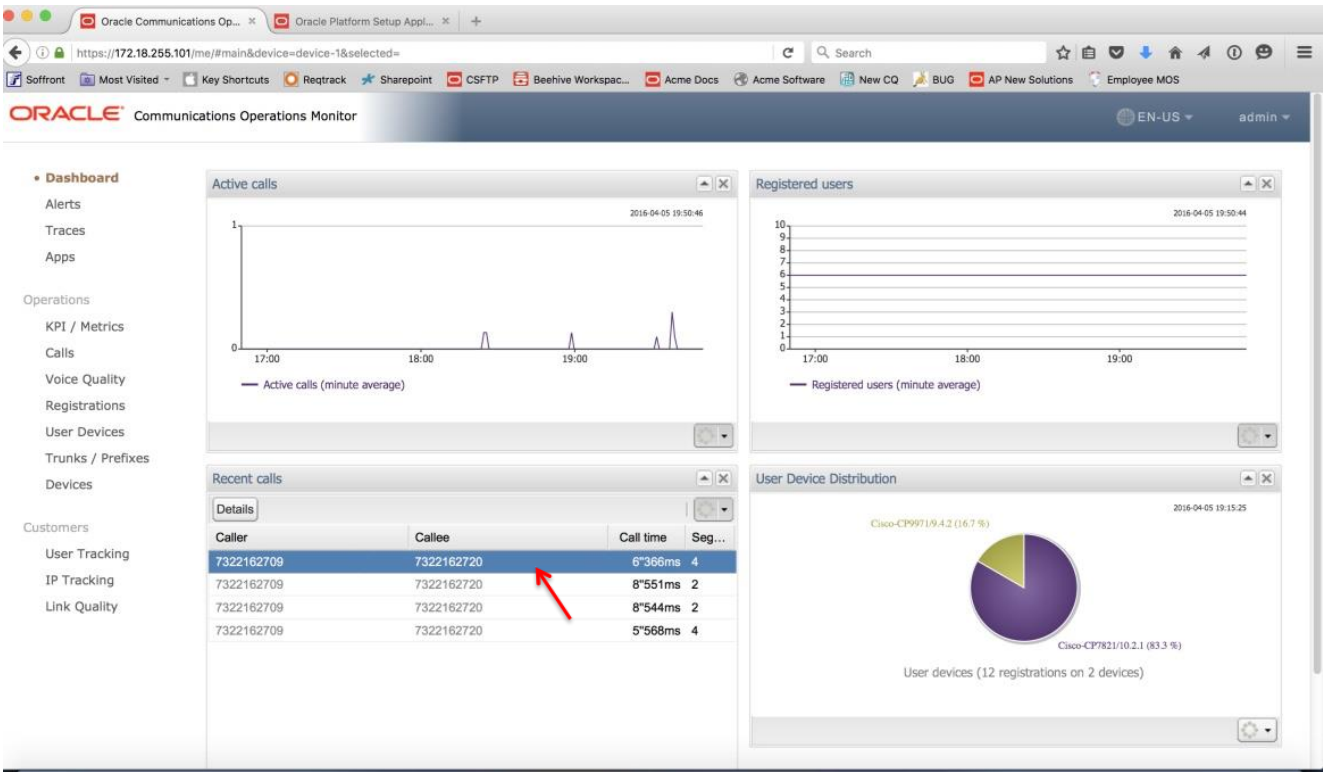


9. Repeat for all other devices in the call flow. Enter each side of the SBC (inside and outside) separately. You don't necessarily need to define the access client's information.

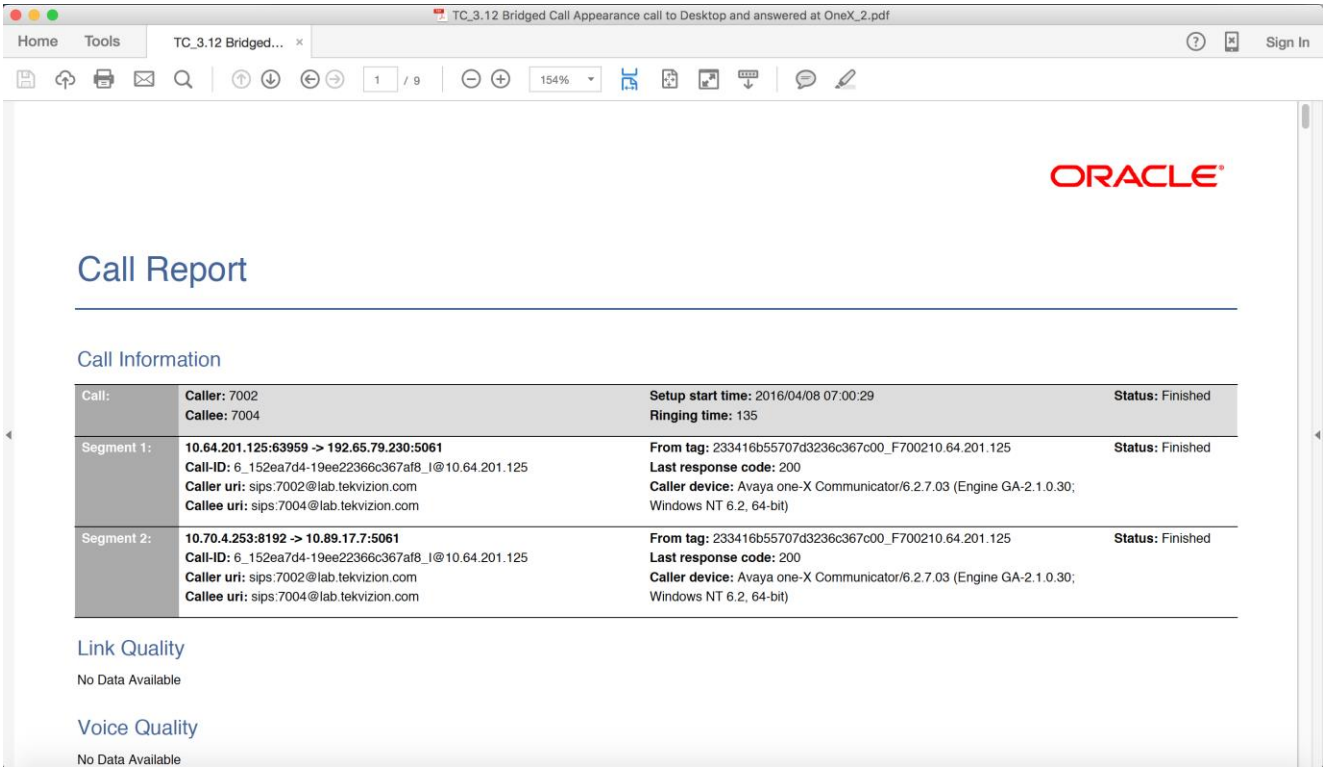
10. On the Dashboard, under Recent Calls, make sure the Auto Refresh is set to something other than Off.



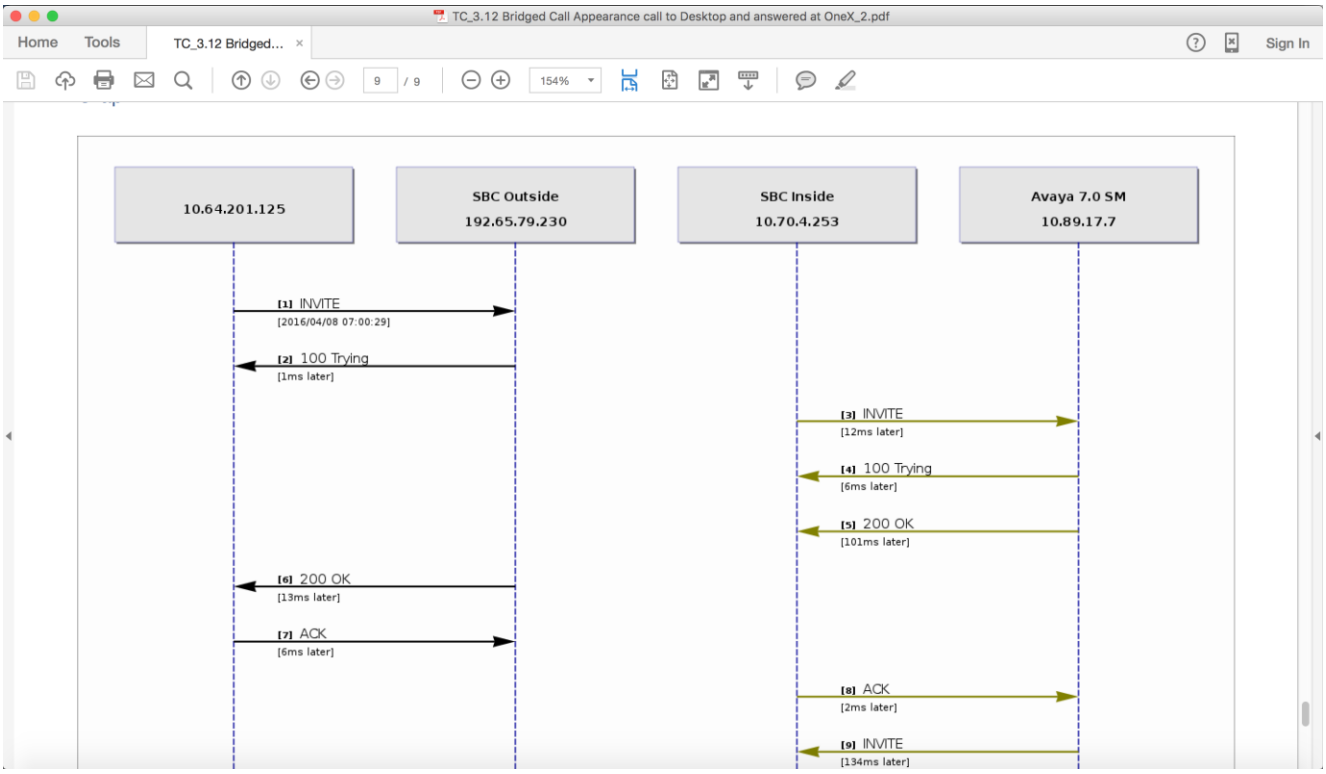
11. Make a call. After the call is finished, the call will show up under Recent Calls with 2 or more segments if the call only traverses the SBC once, or with 4 or more segments if the call traverses the SBC twice. Double click on the call.



12. The call will show up with all segments. Click on the PDF button to generate a report.
13. Click on the Create button.
14. Choose to either save the file or open it.
15. View the Call Report in Acrobat Reader or another program. The report will show all segments of the call.



16. At the end of the report after all the SIP messages, there will be a call flow graph that shows each element in the call.



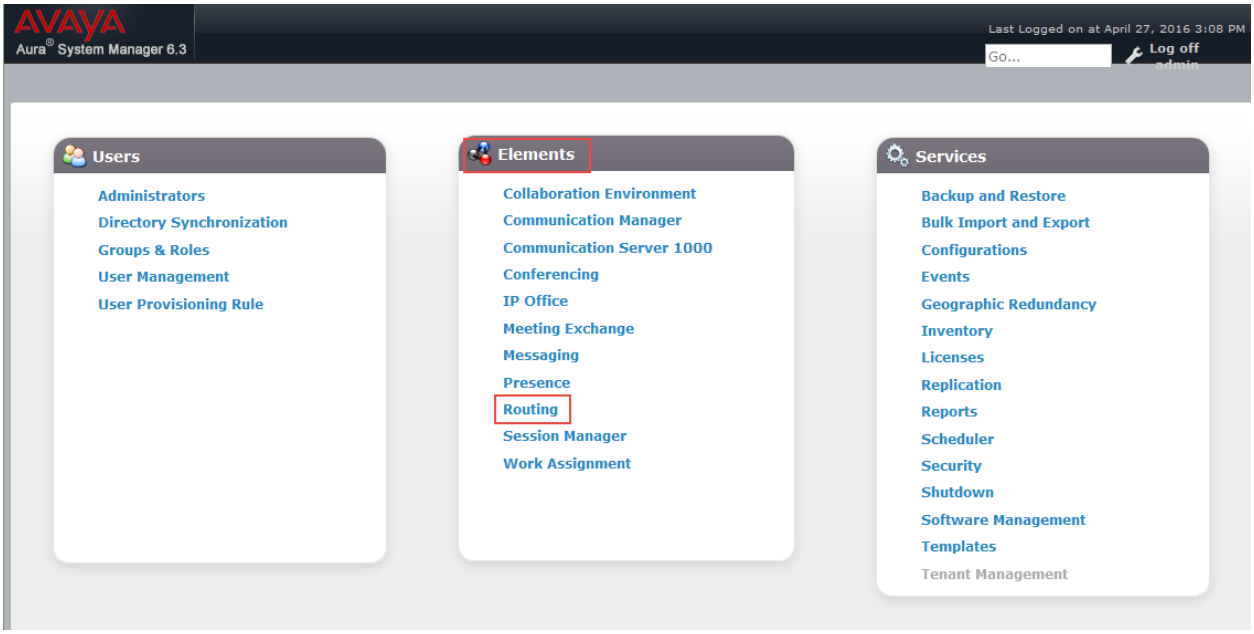
Phase 3 – Configuring the Avaya Session Manager 6.3

The enterprise has a fully functional Avaya Aura System Manager. Configuring the System Manager to operate with the Oracle E-SBC consists of the following steps:

- Adding the E-SBC as a SIP Entity
- Configuring an Entity link between the E-SBC and Session Manager
- Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting
- Enabling Remote Office
- Exporting the System Manager CA Certificate
- Downloading Session Manager's Default Certificate
- Signing the Oracle E-SBC's Certificate on Avaya System Manager
- Installing the System Manager Root Certificate for Endpoints

Adding the E-SBC as a SIP Entity and Configuring an Entity Link

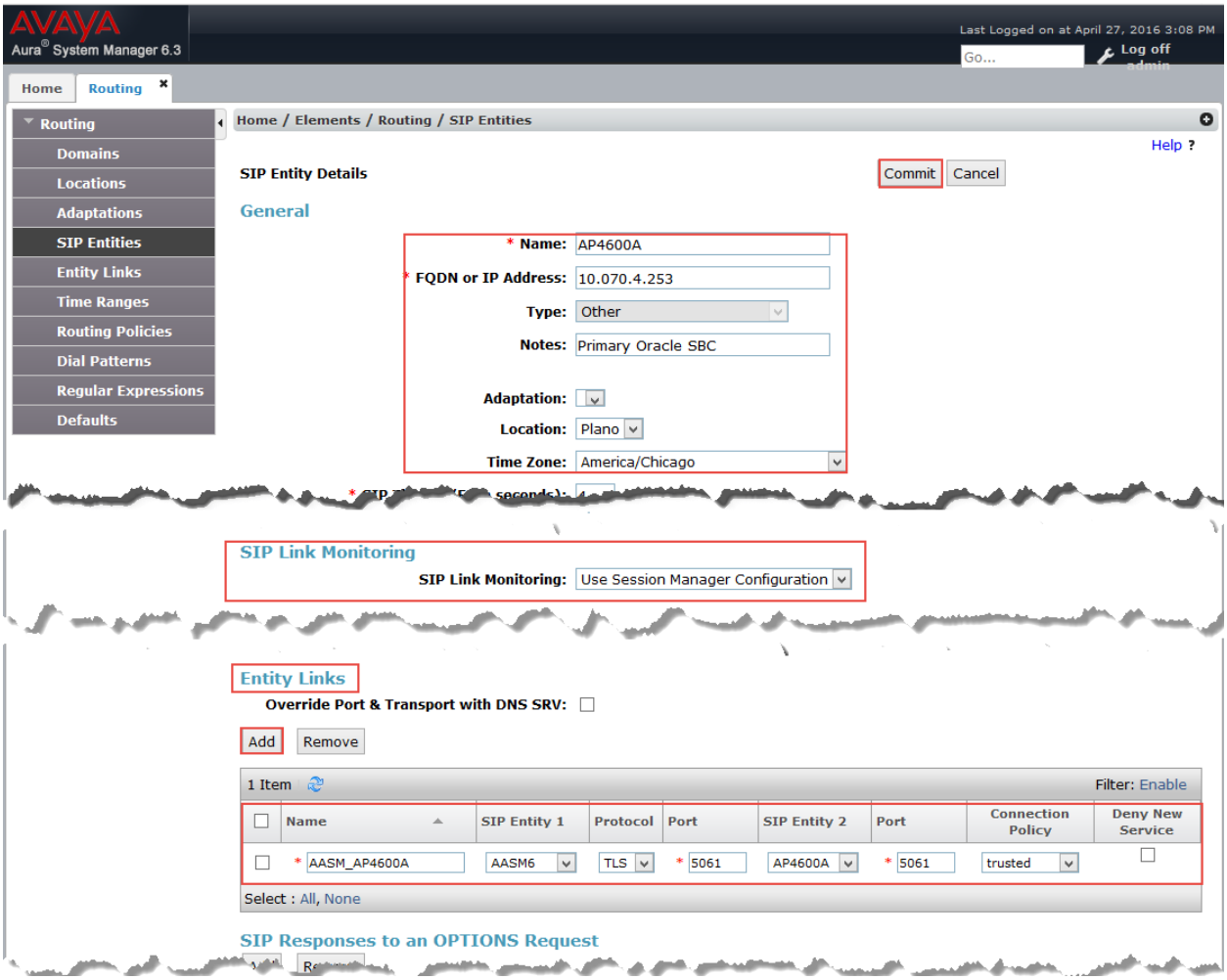
Log in to the Aura System Manager. Click on **Routing** under the **Elements** section.



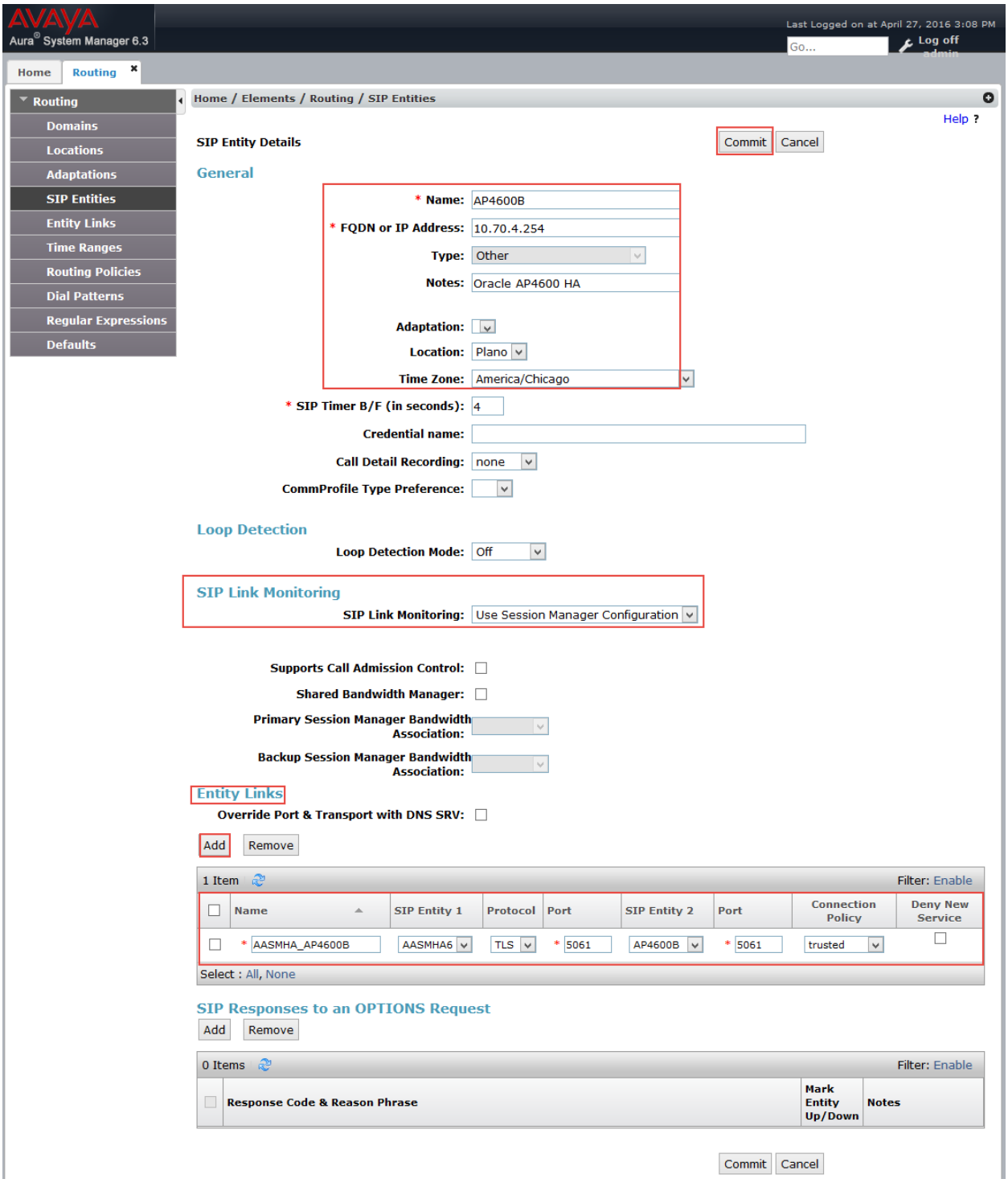
On the **Routing** tab, select **SIP Entities** from the menu on the left side of the screen. Click **New** to add the E-SBC as a SIP entity as shown below.

1. Set **Name**: **AP4600A (example in this configuration)**
2. Set **FQDN or IP Address**: This is the "inside" IP address of Oracle E-SBC, 10.70.4.253 in this example.
3. Set **Type**: **Other**
4. Set **Location**: Select **Plano from drop down (example in this configuration)**
5. Set **Time Zone**: **America/Chicago (example in this configuration)**
6. Under Link Monitoring, select **Use Session Manager Configuration** from the dropdown list
7. Under Entity Links, Click **Add**
   - Set **SIP Entity 1**: Select **AASM6** which was previously configured
   - Set **SIP Entity 2**: leave the default value **AP4600A**
   - Set **Protocol**: **TLS**
   - Set **Ports**: set both Ports to **5061**
   - Set **Connection Policy**: **trusted**
8. Leave all other fields as default values

Click **Commit**



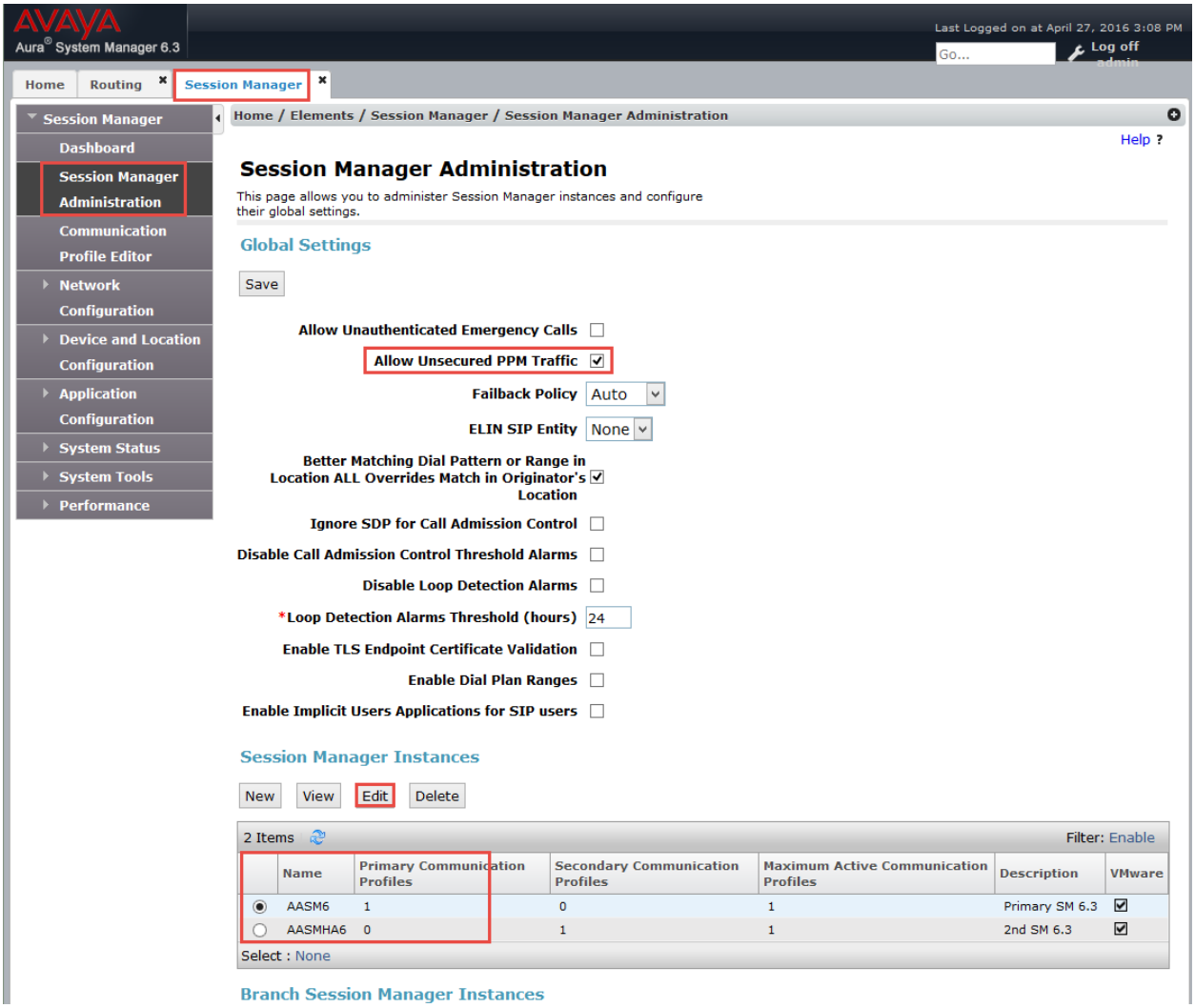
9. Repeat steps 1-8 to configure the SIP Entity for secondary (“B” site) SBC



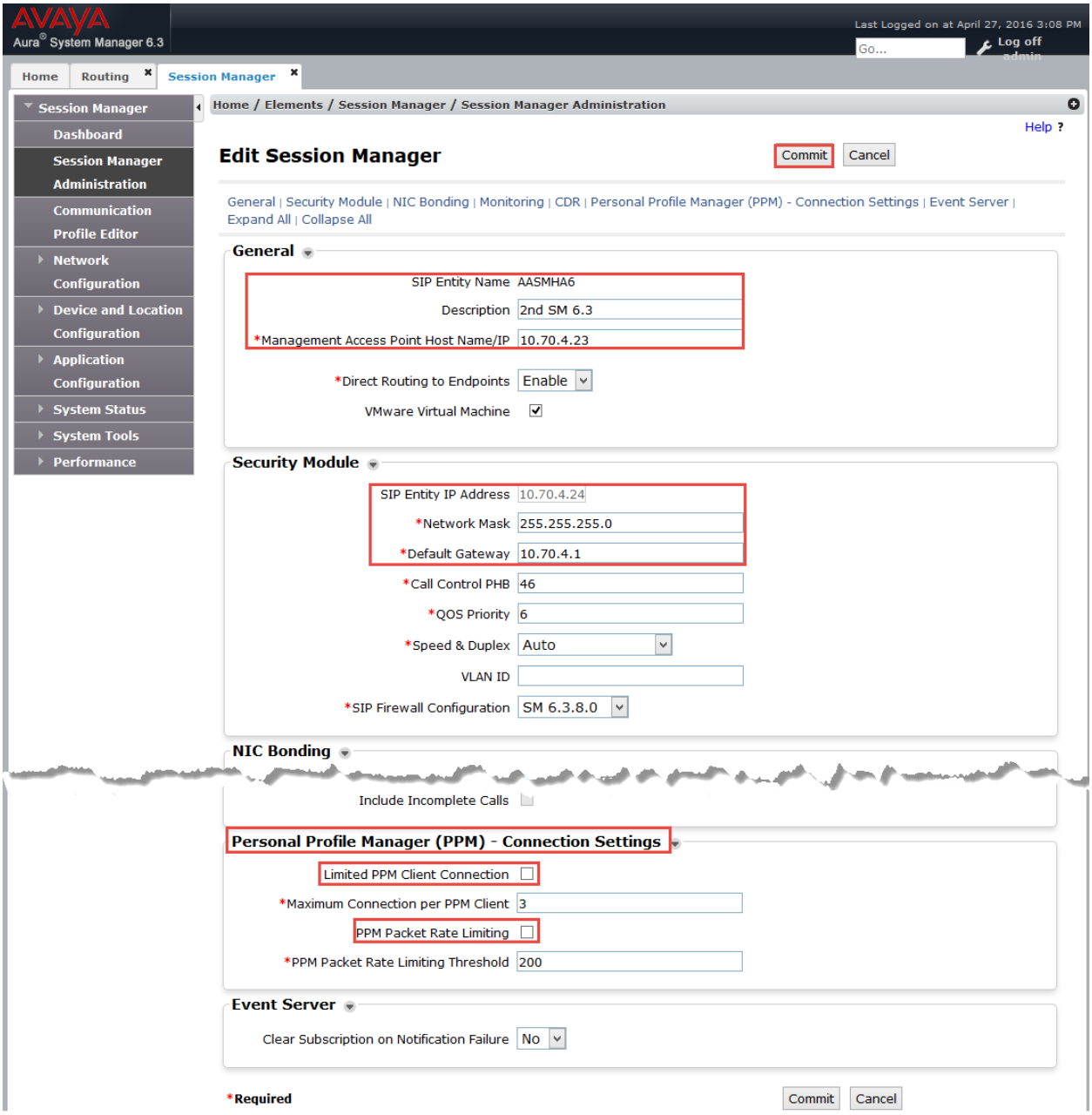
Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

Navigate to: **Elements**->**Session Manager**->**Session Manager Administration**.

1. Set **Allow Unsecured PPM Traffic**: **checked.** Note that this is only required if you’re using HTTP for the PPM downloads. If you’re using HTTPS as shown in the E-SBC configuration, leave this unchecked.
2. Select the proper Session Manager instance and click **Edit**



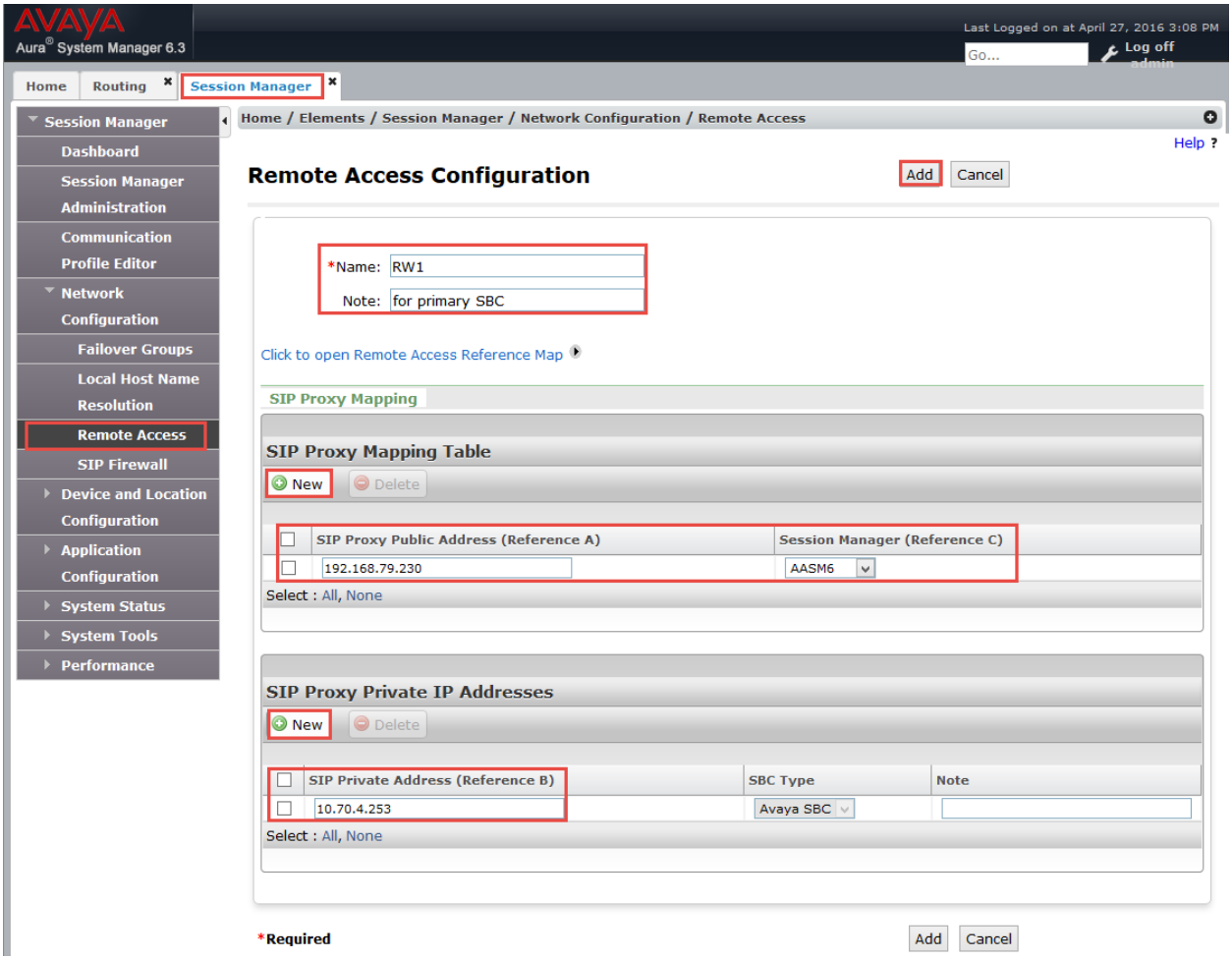
3. Scroll down to **PPM – Connection Settings**
   - Set **Limited PPM Client Connection**: **unchecked**
   - Set **PPM Packet Rate Limiting**: **unchecked**
4. Leave all other fields as default
5. Click **Commit**
6. Repeat steps 2-5 for secondary "B" site SBC
7. Click **Save** at the Session Manager Administration page



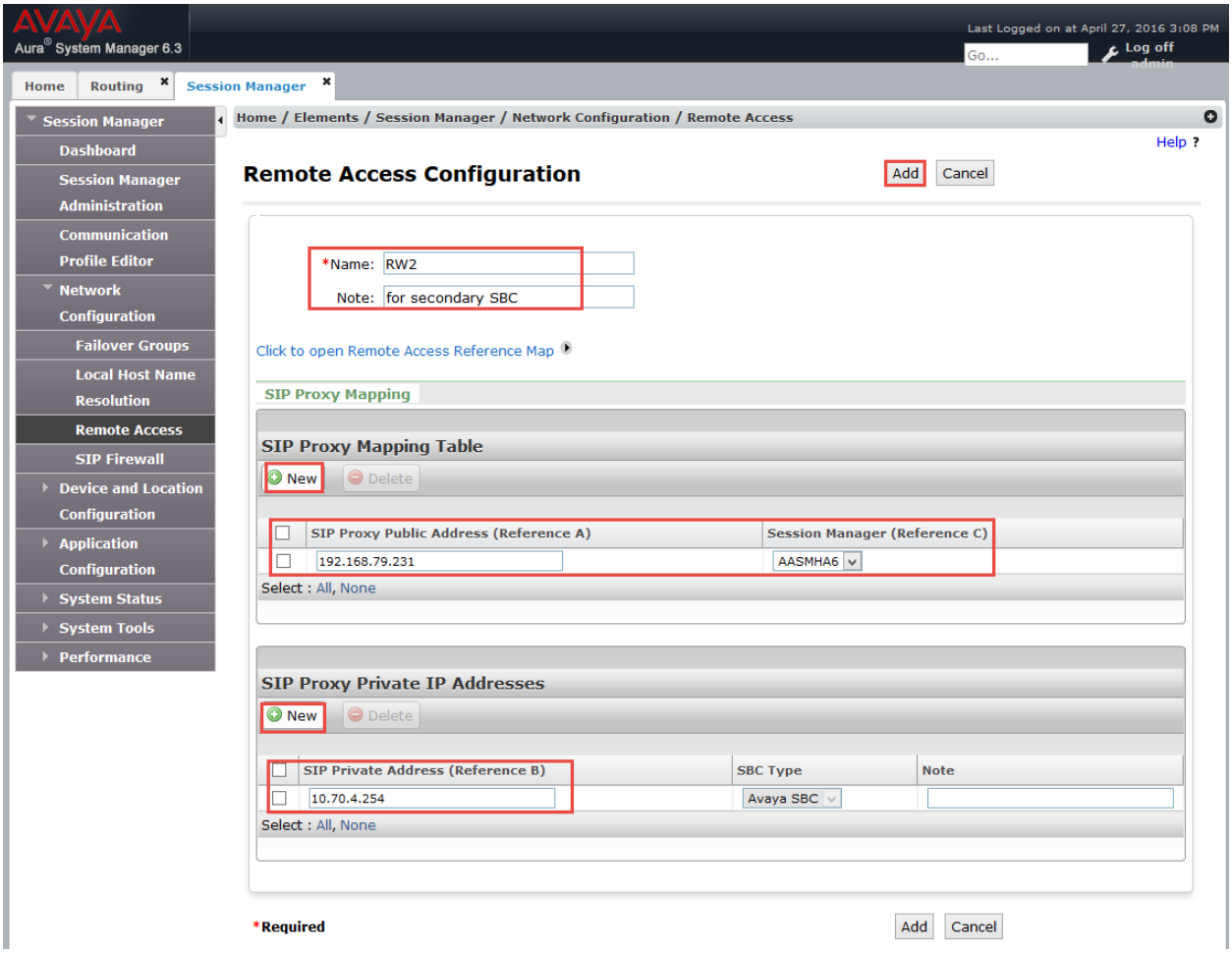
Enabling Remote Office

Navigate to: **Elements**->**Session Manager**->**Network Configuration**->**Remote Access**, Click **New**

1. Set **Name**: **RW1** for this setup.
2. Click **New** under **SIP Proxy Mapping Table**. Add the Oracle SBC outside interface IP address for **SIP Proxy Public Address**, 192.168.79.230 is given in this example.
3. Click **New** under **SIP Proxy Private IP Address**. Add the Oracle SBC inside interface IP address for **SIP Private Address**, 10.70.4.253 is given in this example.
4. Click **Add.**



5. Repeat steps 1-4 for the secondary “B” site SBC.

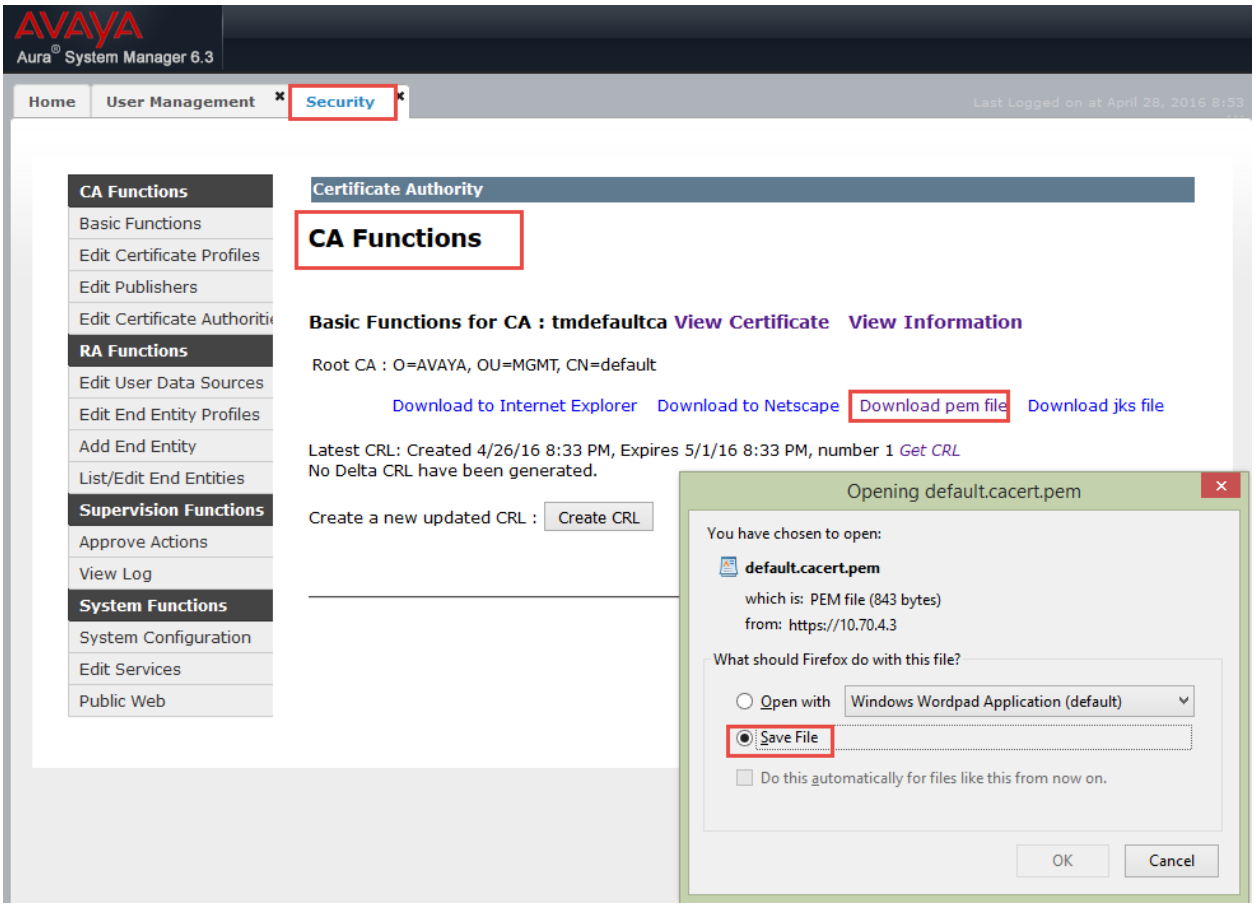


Exporting the System Manager CA Certificate

In this lab setup, the Avaya Aura System Manager acts as the Certificate Authority (CA). You must install the System Manager trusted root certificates on endpoints that communicate with Session Manager over TLS.

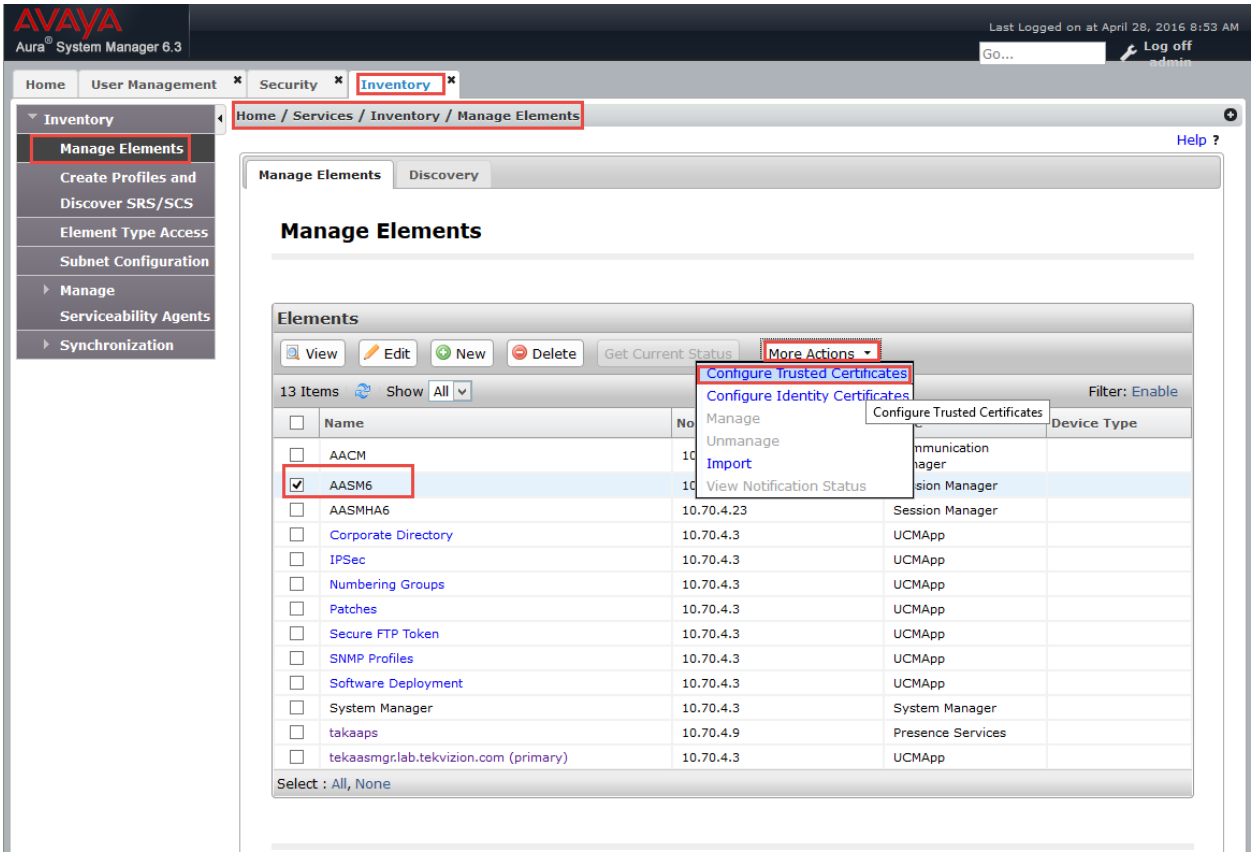
On the home page of System Manager Web Console,

1. Navigate to: **Services->Security->Certificate**
2. Click **Download PEM file**
3. Select **Save File**
4. Click **OK**

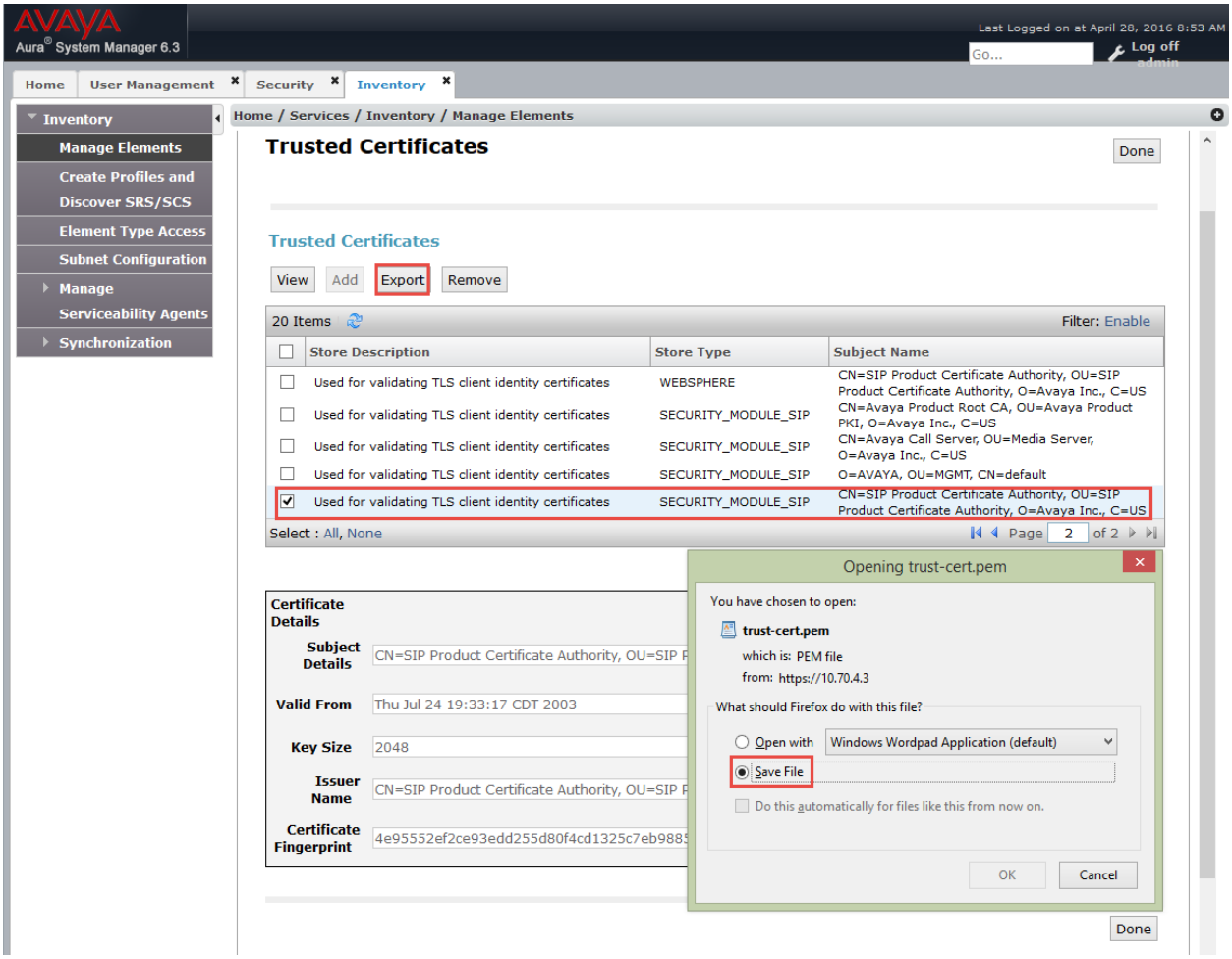


Downloading Session Manager Default Certificate

1. Navigate to **Services**->**Inventory**->**Manage Element**
2. Select the proper Session Manager**, AASM6** is selected for this setup
3. Click **More Actions**
4. Select **Configure Trusted Certificates**



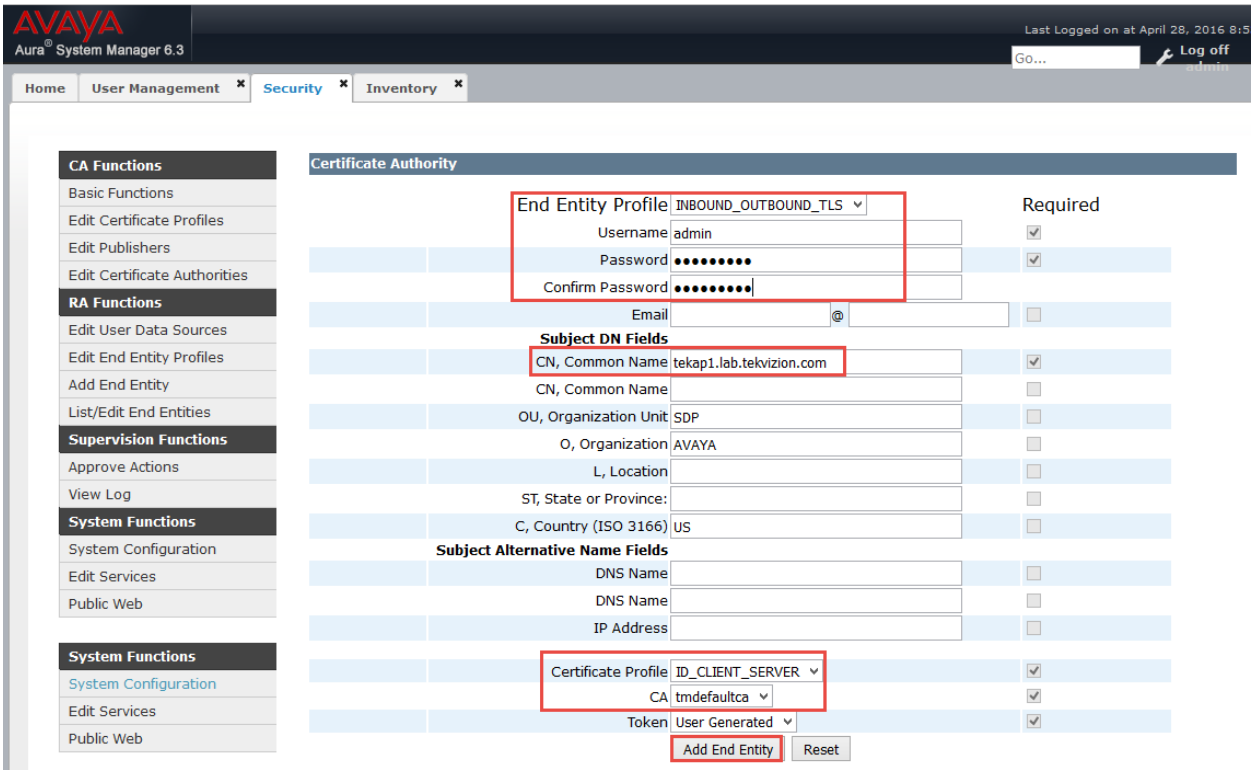
5. Click **Export**
6. Save the file



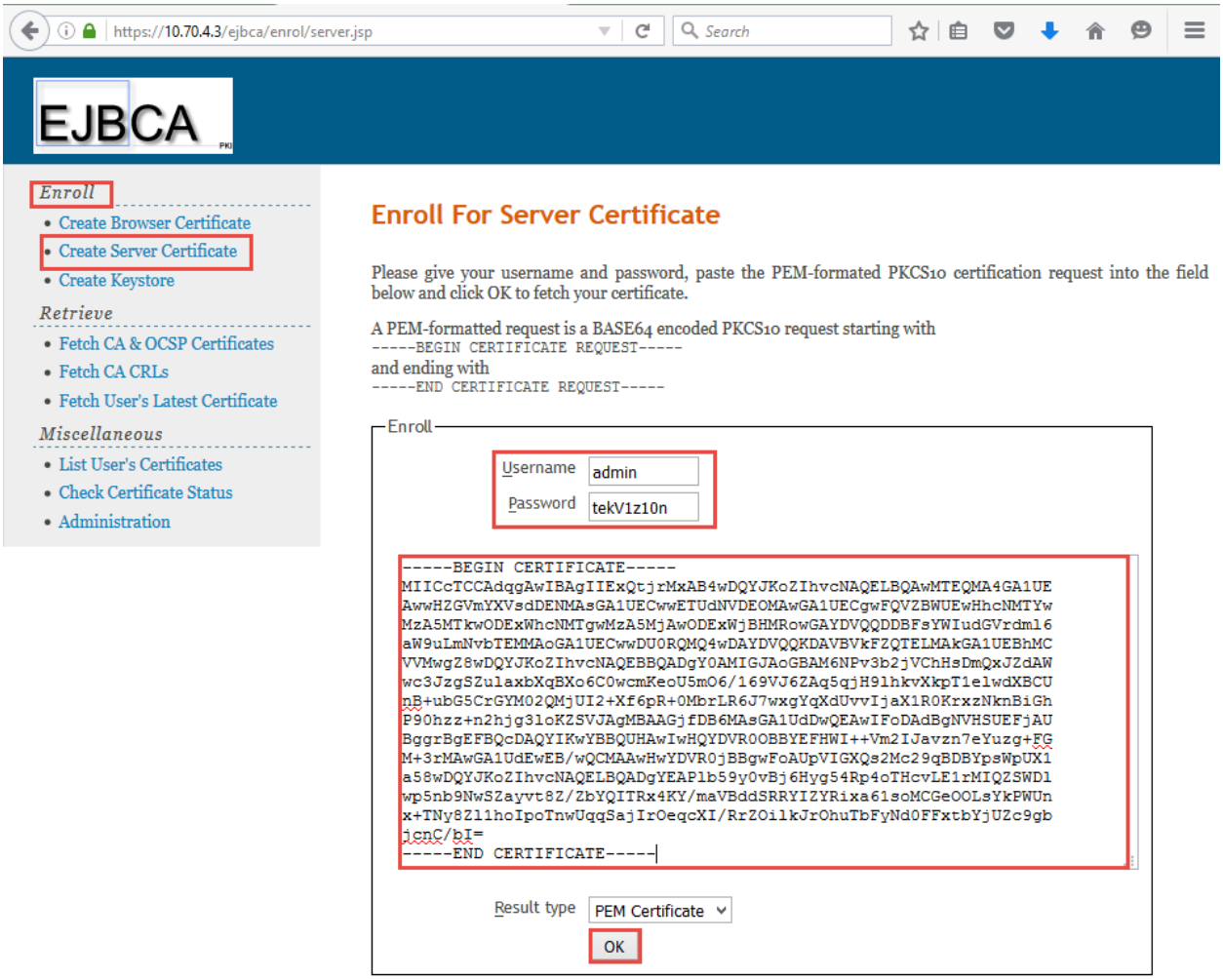
7. Repeat the steps for secondary Session Manager

Signing the Oracle E-SBC's Certificate on Avaya System Manager

1. Login to the System Manger web Console
2. Navigate to: **Services**->**Security**->**Certificate**->**Authority**->**Add End Entity**
3. Set **Entity Profile**: Select **INBOUND_OUTBOUND_TLS** from drop down
4. Set **Username**: **admin** is used for this setup
5. Set **Password**: enter the password here
6. Set **CN, Common Name**: The Oracle SBC FQDN **tekap1.lab.tekvizion.com** is used here
7. Leave all other fields as default
8. Click **Add End Entity**



9. Navigate to: **Services->Security->Certificate->Authority->Public Web**
10. Under **Enroll**, click **Create Server Certificate.**
11. Set **Username**: previously configured **admin** is input here.
12. Set **Enrollment code**: the password configured in previous step is given here.
13. Paste the Certificate Signing Request from the Oracle E-SBC and click **OK.**
14. Save the certificate.
15. Import the certificate into the E-SBC as described in the “Importing the SBC’s Signed Certificates” section above.



16. Repeat steps 2-15 for the secondary “B” site E-SBC.

Installing System Manager’s Root Certificate for Endpoints

Avaya desk phones will download the System Manager root certificate while they reboot. In order to make the One-X Communicator and One-X Communicator for Mobile work, the System Manager’s root certificate needs to be installed as a trusted root certificate on the PC and mobile phones (Android or IOS) that are running One-X Communicator for TLS to work with the Oracle E-SBC.

The Avaya System Manager 6.3 is now configured to operate with the E-SBC at the A and B sites.

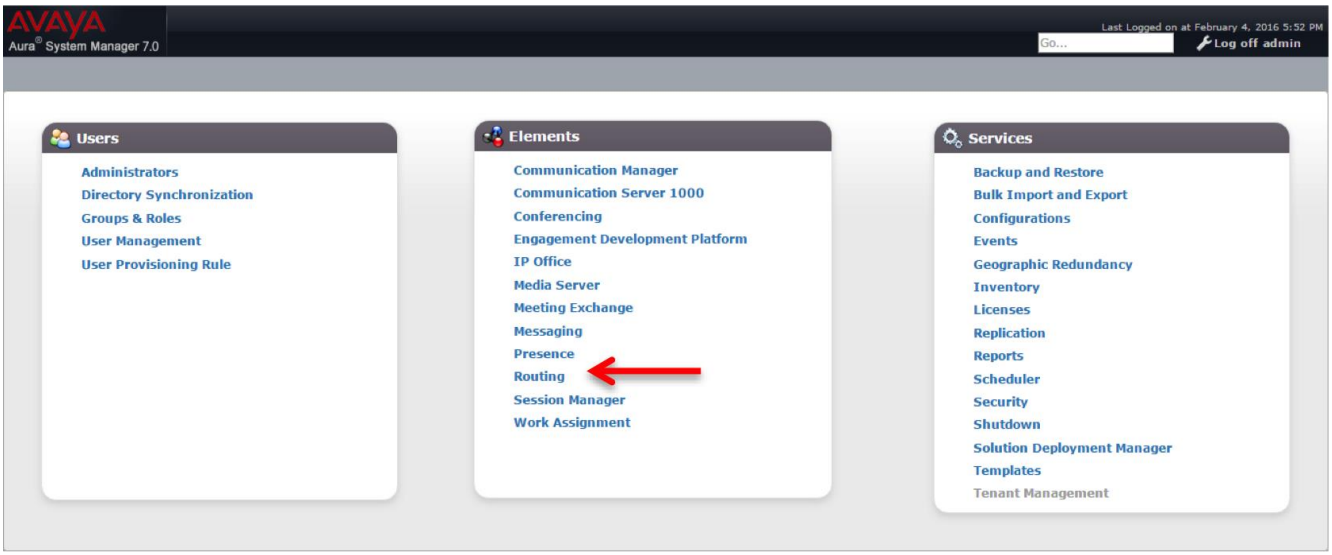
Phase 4 – Configuring the Avaya Session Manager 7.0

The enterprise has a fully functional Avaya Aura System Manager. Configuring the System Manager to operate with the Oracle E-SBC consists of the following steps:

- Adding the E-SBC as a SIP Entity
- Configuring an Entity link between the E-SBC and Session Manager
- Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting
- Enabling Remote Office
- Exporting the System Manager CA Certificate
- Replacing Session Manager's Identity Certificate
- Signing the Oracle E-SBC's Certificate on Avaya System Manager
- Downloading Session Manager's Default Certificate
- Installing the System Manager Root Certificate for Endpoints

Adding the E-SBC as a SIP Entity and Configuring an Entity Link

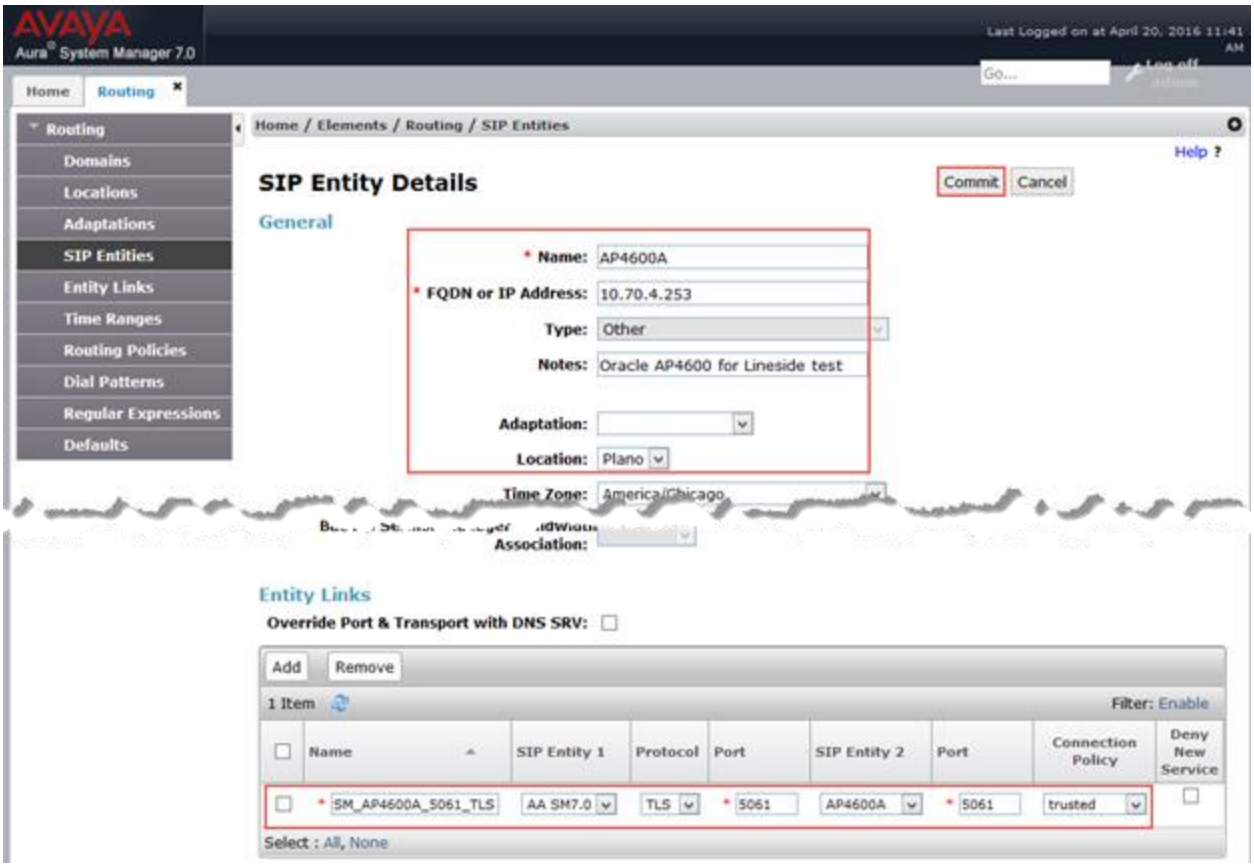
Log in to the Aura System Manager. Click on **Routing** under the **Elements** section.



On the **Routing** tab, select **SIP Entities** from the menu on the left side of the screen. Click **New** to add the E-SBC as a SIP entity as shown below.

10. Set **Name**: **AP4600A (example in this configuration)**
11. Set **FQDN or IP Address**: This is the "inside" IP address of Oracle E-SBC, 10.70.4.253 in this example.
12. Set **Type**: **Other**
13. Set **Location**: Select **Plano from drop down (example in this configuration)**
14. Set **Time Zone**: **America/Chicago (example in this configuration)**
15. Under Link Monitoring, select **Link Monitoring Enabled** from the dropdown list
16. Under Entity Links, Click **Add**
    - Set **SIP Entity 1**: Select **AA SM7.0** which was previously configured
    - Set **SIP Entity 2**: leave the default value **AP4600A**
    - Set **Protocol**: **TLS**
    - Set **Ports**: set both Ports to **5061**
    - Set **Connection Policy**: **trusted**
17. Leave all other fields as default values

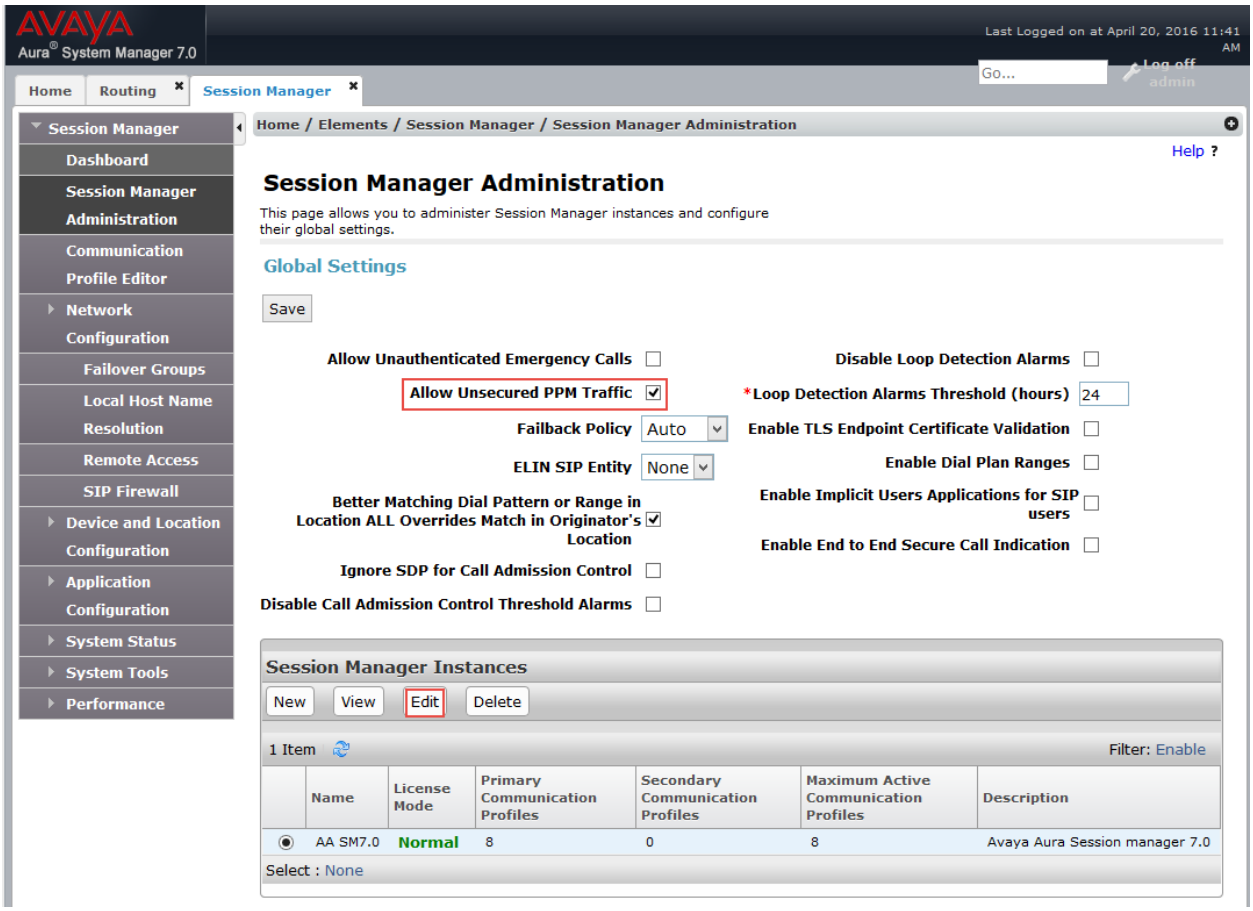
Click **Commit**



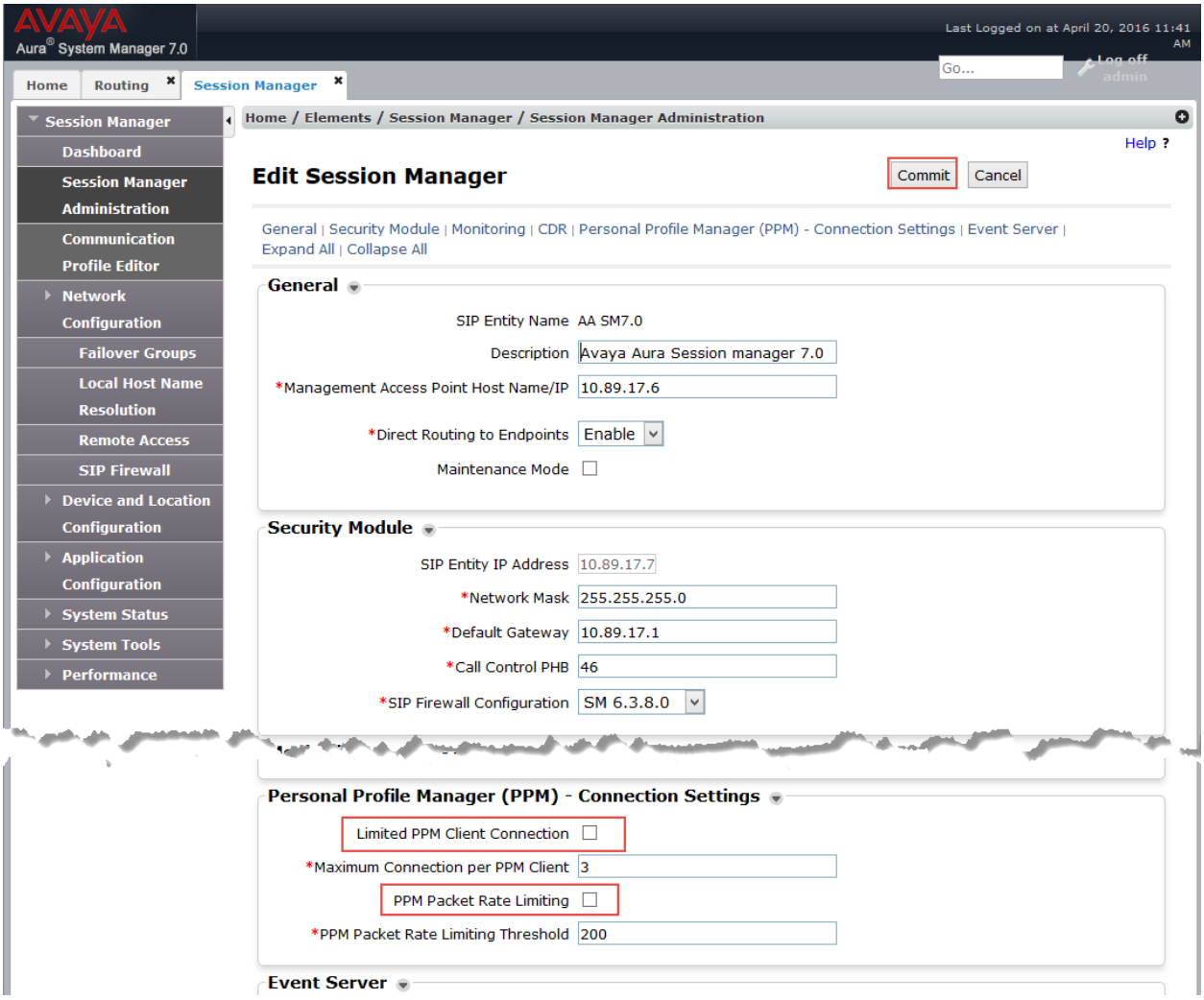
Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

Navigate to: **Elements**->**Session Manager**->**Session Manager Administration**.

8. Set **Allow Unsecured PPM Traffic**: **checked.** Note that this is only required if you're using HTTP for the PPM downloads. If you're using HTTPS as shown in the E-SBC configuration, leave this unchecked.
9. Select the proper Session Manager instance and click **Edit**



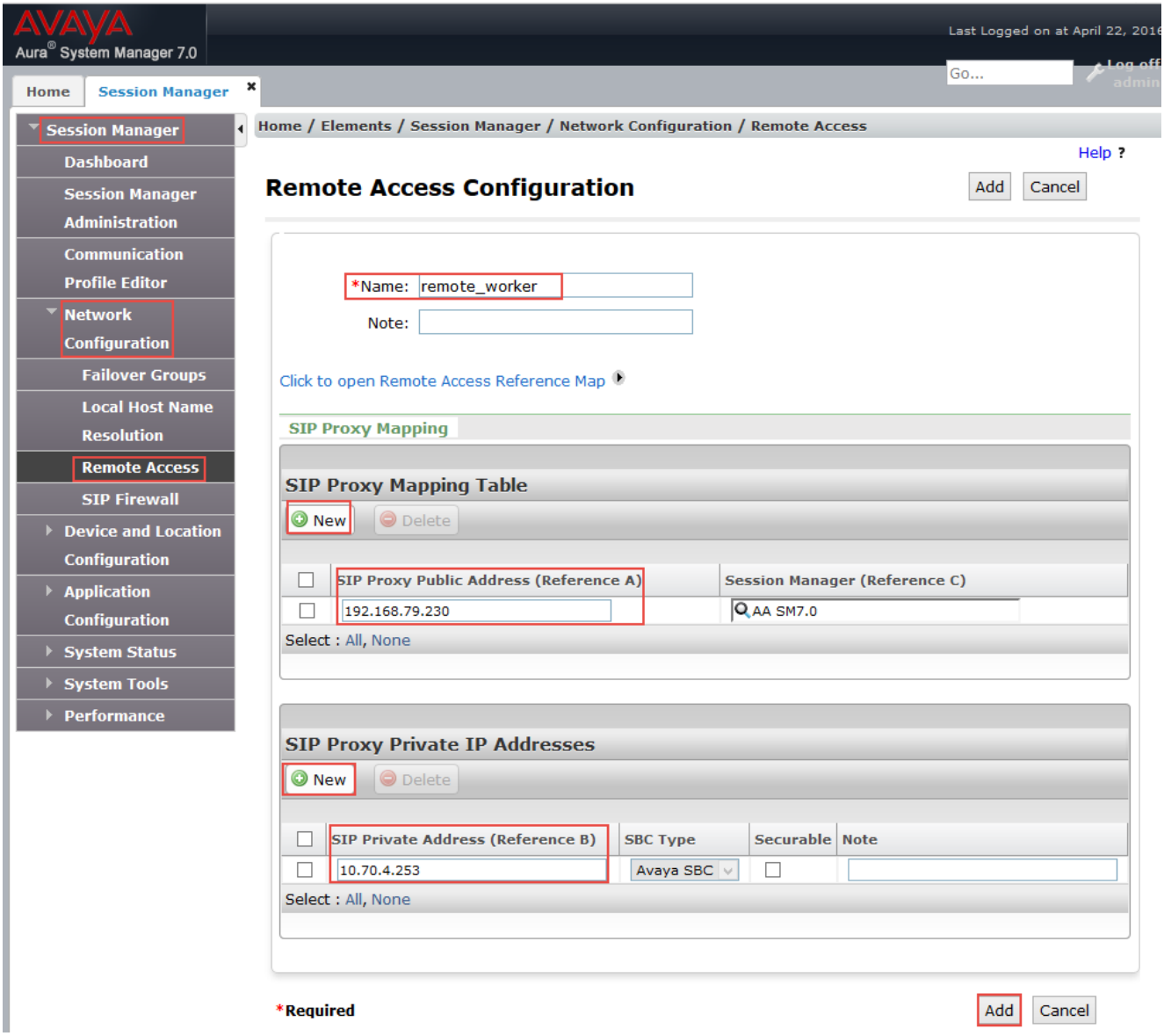
10. Scroll down to **PPM – Connection Settings**
    - Set **Limited PPM Client Connection**: **unchecked**
    - Set **PPM Packet Rate Limiting**: **unchecked**
11. Leave all other fields as default
12. Click **Commit**
13. Click **Save** at the Session Manager Administration page



Enabling Remote Office

Navigate to: **Elements**->**Session Manager**->**Network Configuration**->**Remote Access**, Click **New**

6. Set **Name**: **remote_worker** for this setup.
7. Click **New** under **SIP Proxy Mapping Table**. Add the Oracle SBC outside interface IP address for **SIP Proxy Public Address**, 192.168.79.230 is given in this example.
8. Click **New** under **SIP Proxy Private IP Address**. Add the Oracle SBC inside interface IP address for **SIP Private Address**, 10.70.4.253 is given in this example.
9. Click **Add.**

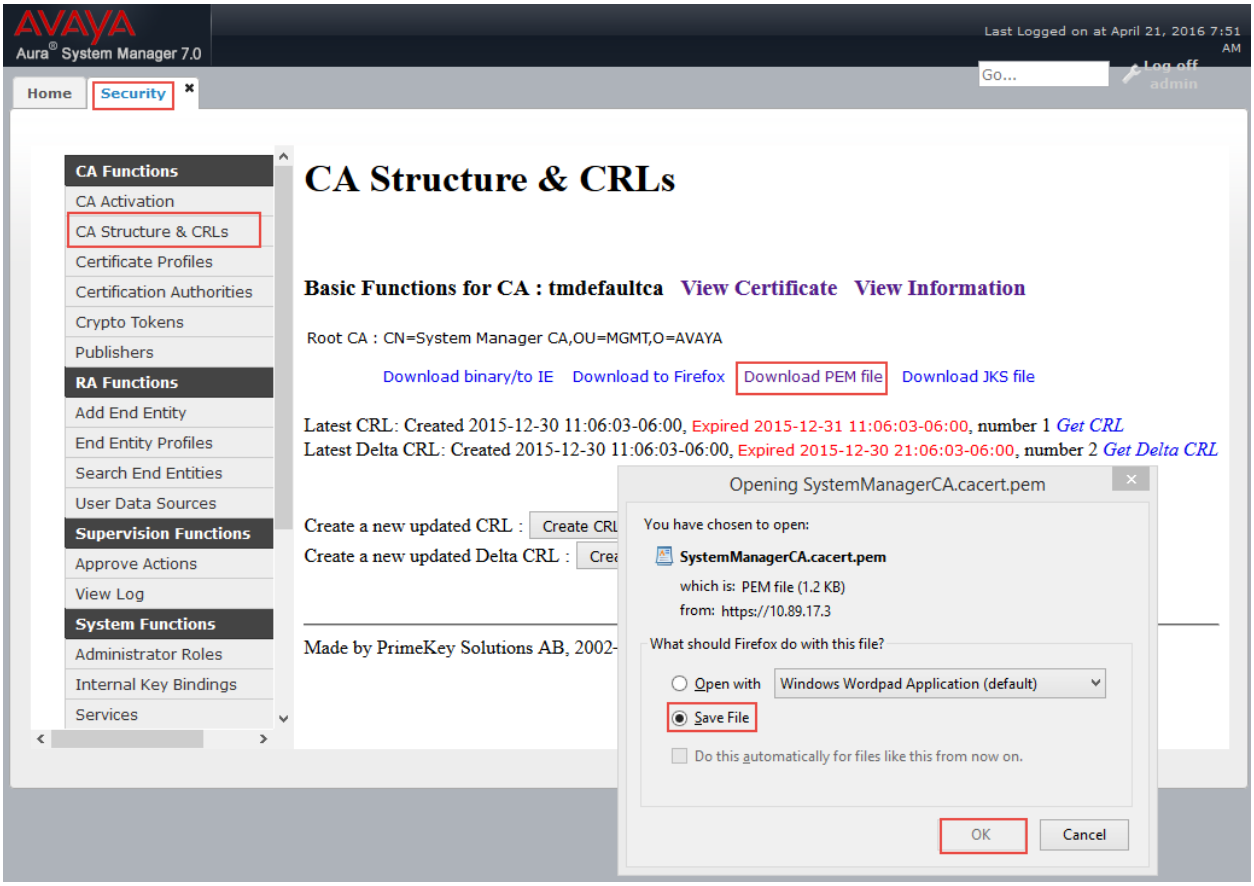


Exporting the System Manager CA Certificate

In this lab setup, the Avaya Aura System Manager acts as the Certificate Authority (CA). You must install the System Manager trusted root certificates on endpoints that communicate with Session Manager over TLS.

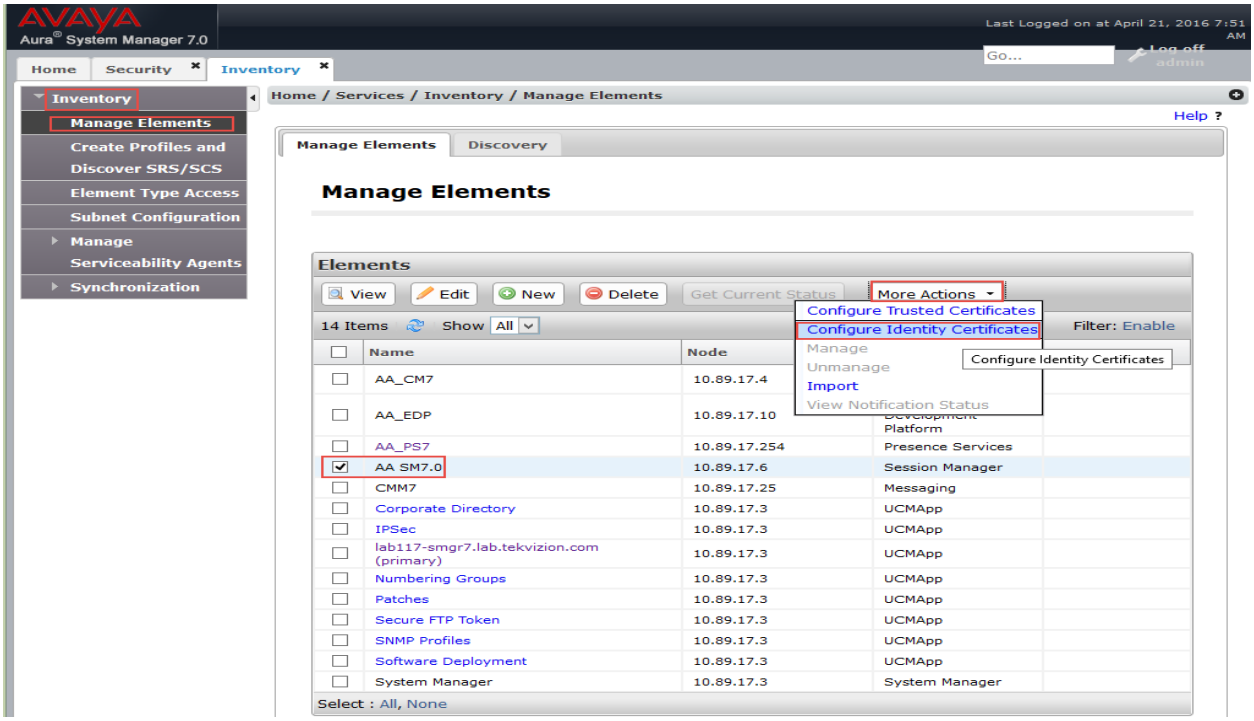
On the home page of System Manager Web Console,

5. Navigate to: **Services->Security->Certificate->Authority->CA Structure & CRLs**
6. Click **Download PEM file**
7. Select **Save File**
8. Click **OK**

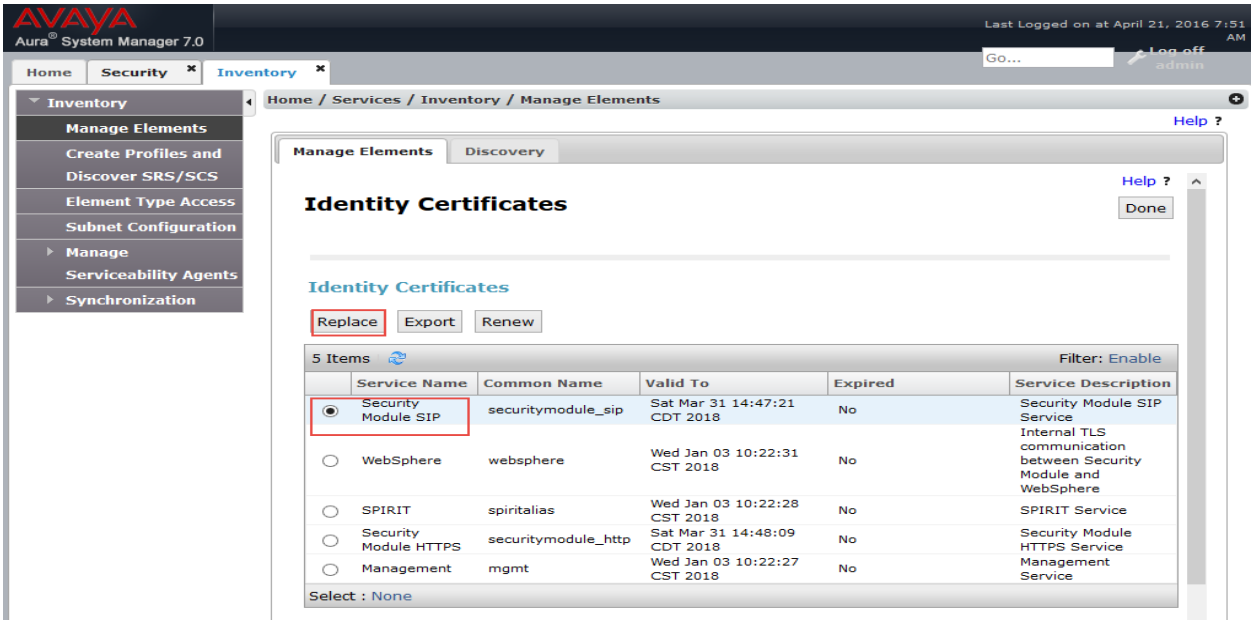


Replacing Session Manager's Identity Certificate

8. Navigate to **Services**->**Inventory**->**Manage Element**
9. Select the proper Session Manager**, AA SM7.0** is selected for this setup
10. Click **More Actions**
11. Select **Configure Identity Certificate**

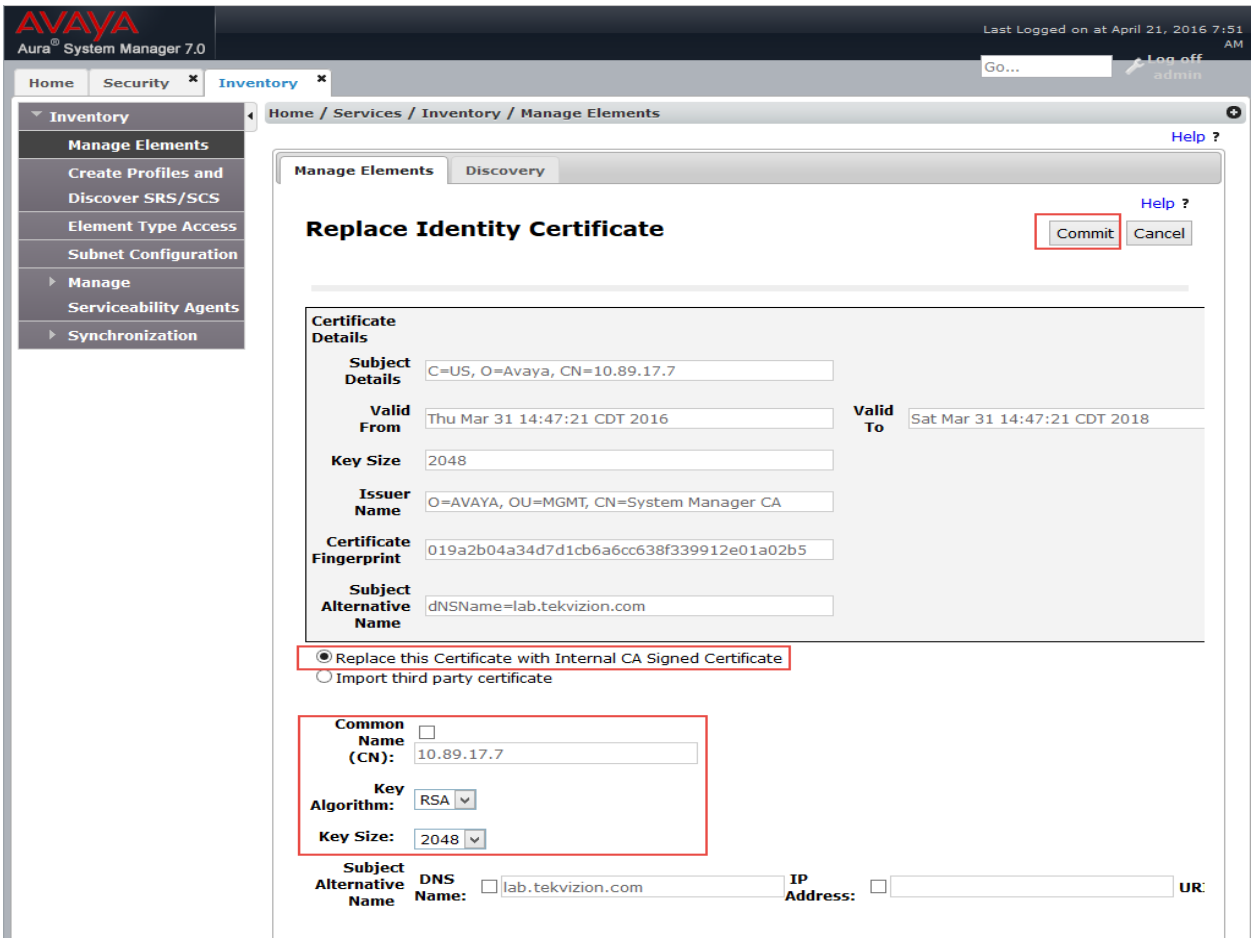


12. Select Security Module SIP
13. Click Replace



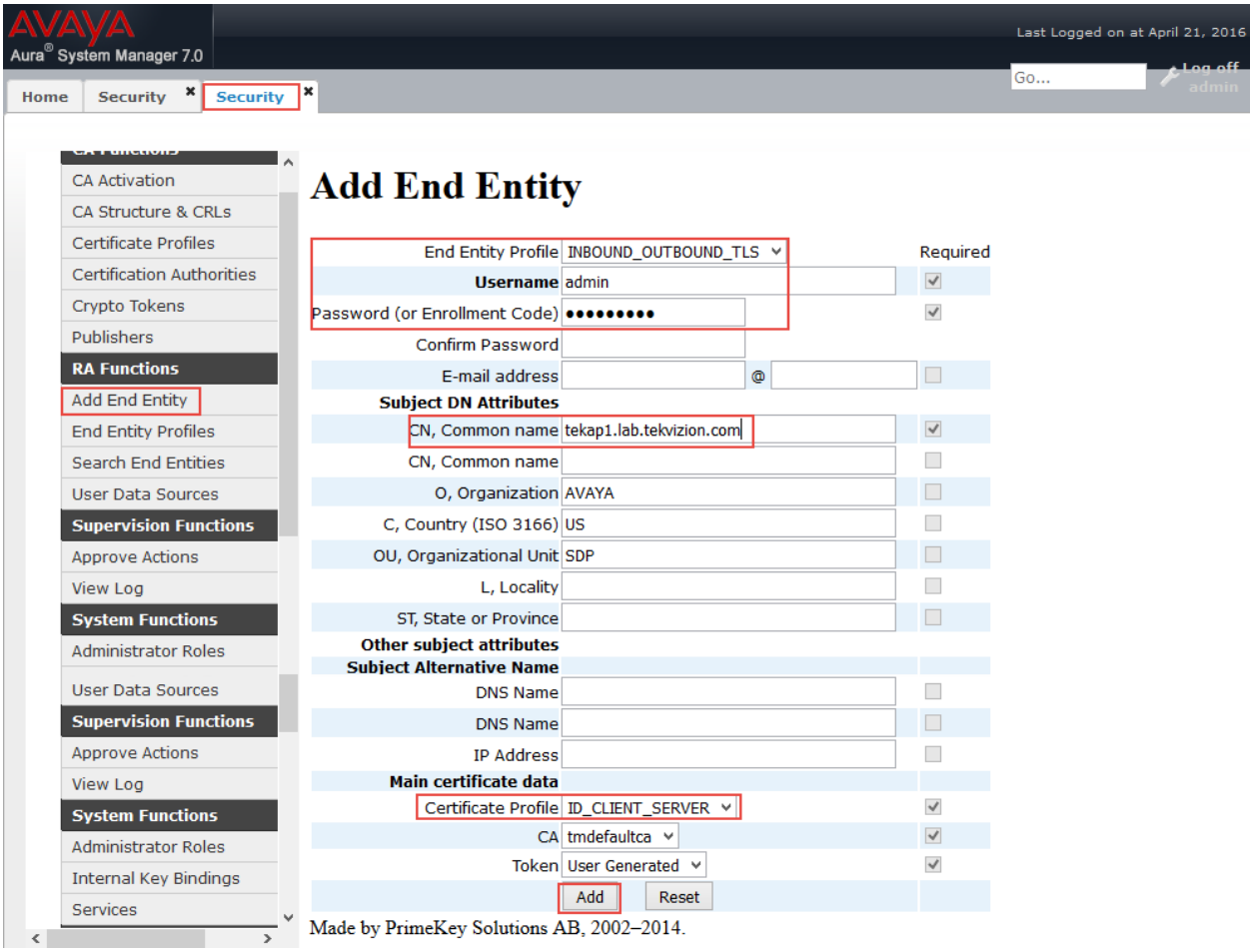
14. Check **Replace this Certificate with Internal CA signed Certificate**
15. Set **Common Name**: Session Manager SIP IP address 10.89.17.7 is given here
16. Set **Key Algorithm: RSA** is selected from drop down

17. **Set Key Size: 2048** is selected for the setup
18. Click **Commit**
19. Repeat same procedures for Security Module HTTPS

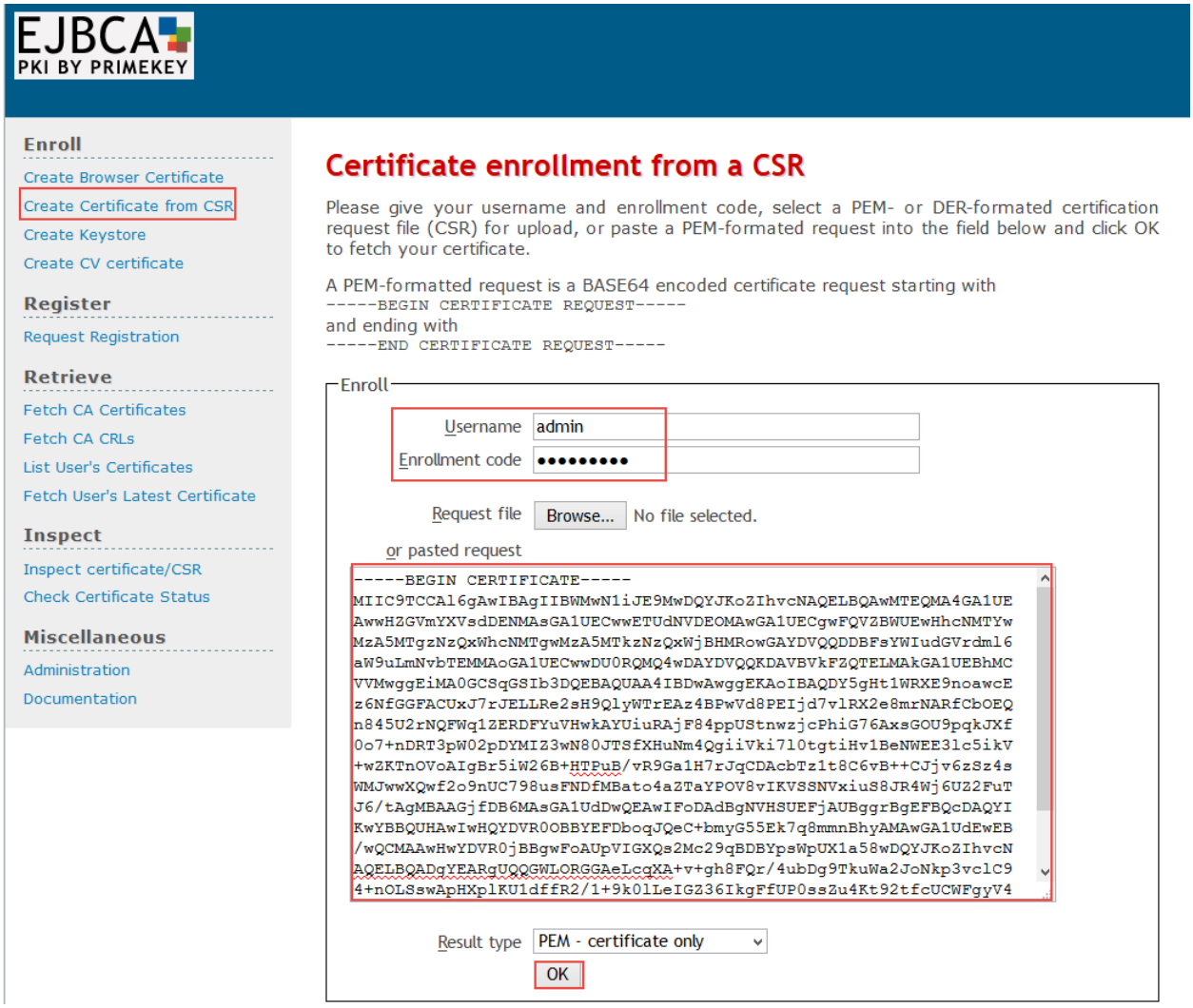


Signing the Oracle E-SBC's Certificate on Avaya System Manager

17. Login to the System Manger web Console
18. Navigate to: **Services**->**Security**->**Certificate**->**Authority**->**Add End Entity**
19. Set **Entity Profile**: Select **INBOUND_OUTBOUND_TLS** from drop down
20. Set **Username**: **admin** is used for this setup
21. Set **Password**: enter the password here
22. Set **CN, Common Name**: The Oracle SBC FQDN **tekap1.lab.tekvizion.com** is used here
23. Leave all other fields as default
24. Click **Add**



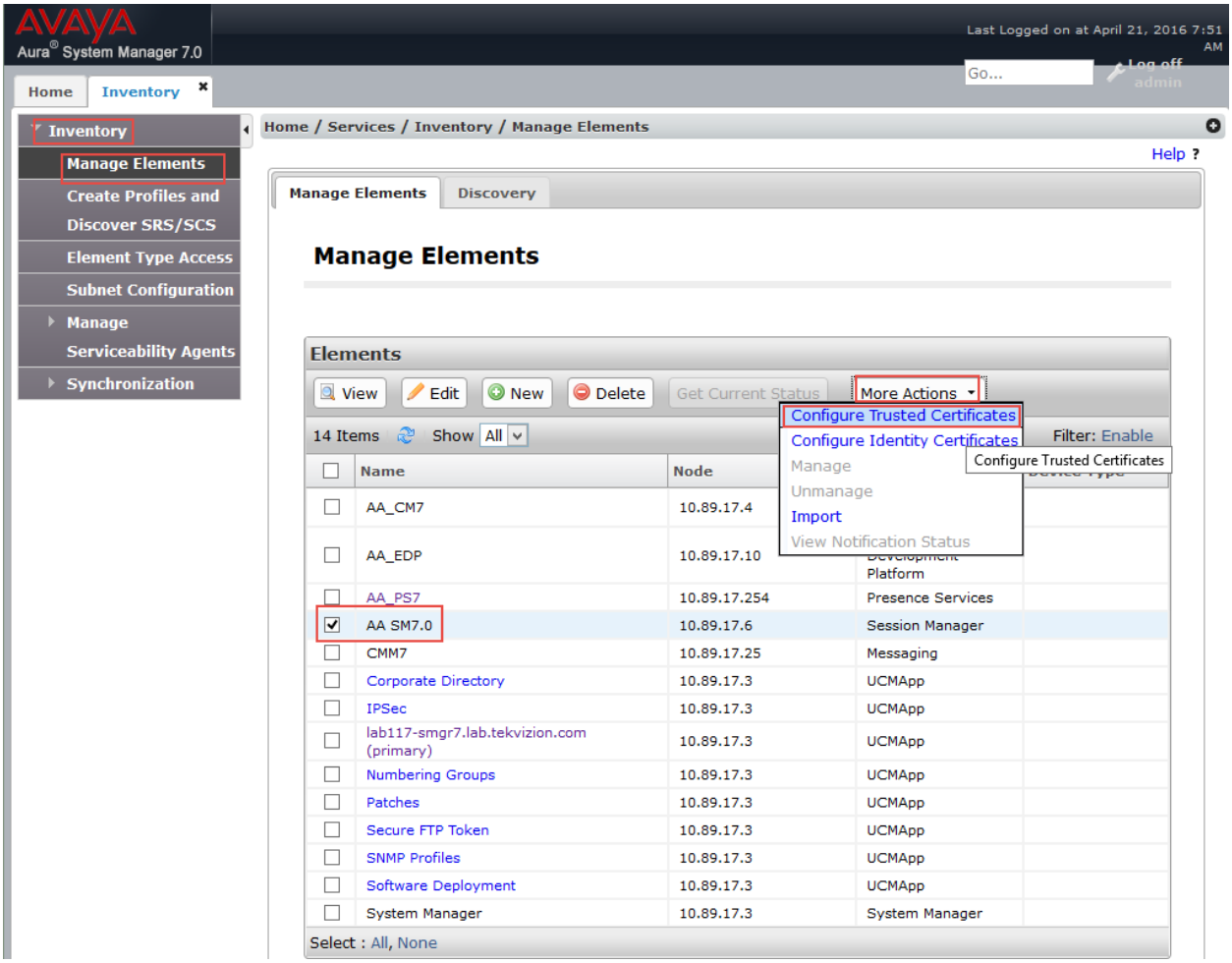
25. Click **Public Web** on the left Panel. A new web page appears.
26. Under **Enroll**, click **Create Certificate from CSR.**
27. Set **Username**: previously configured **admin** is input here.
28. Set **Enrollment code**: the password configured in previous step is given here.
29. Paste the Certificate Signing Request from the Oracle E-SBC and click **OK.**
30. Save the certificate.
31. Import the certificate into the E-SBC as described in the "Importing the SBC's Signed Certificates" section above.



Downloading Session Manager's Default Certificate

From the System Manager Web Console

1. Navigate to: **Services**->**Inventory**->**Manage Elements**
2. Select the proper Session Manager, **AA SM7.0** is for this setup
3. Click **More Actions**
4. Select **Configure Trusted Certificates**



5. Select the Certificate with **CN=SIP Product certificate Authority for SECURITY_MODULE_SIP**
6. Click **Export**
7. Save the file

Installing System Manager's Root Certificate for Endpoints

Avaya desk phones will download the System Manager root certificate while they reboot. In order to make the One-X Communicator and One-X Communicator for Mobile work, the System Manager's root certificate needs to be installed as a trusted root certificate on the PC and mobile phones (Android or IOS) that are running One-X Communicator for TLS to work with the Oracle E-SBC.

The Avaya System Manager 7.0 is now configured to operate with the E-SBC.

Test Plans & Results

Test Plans

The testing was performed by tekVizion.

The test plans consisted of the following test cases.

Avaya 6.3 Test Plan

External ID	External Test Case Type	Title	Description	Status (Pass or Fail etc)
1.1	General	Register / Keep Alive	Register Avaya SIP desktop phone to Avaya Session manager via Oracle SBC	PASS
1.2	General	Register / Keep Alive	Register One-X communicator to Avaya Session manager via Oracle SBC	PASS
1.3	General	Register / Keep Alive	Register One-X Mobile SIP (for IOS or Android) to Avaya Session manager via Oracle SBC	PASS
2.1	Basic Calls	Outbound call	Call from Remote Worker to other users, caller hangs up after call	PASS
2.2	Basic Calls	Outbound call	Call from Remote Worker to other users, called party hangs up after call	PASS
2.3	Basic Calls	Inbound call	Call to Remote Worker from other user, calling party hangs up	PASS
2.4	Basic Calls	Inbound call	Call to Remote Worker from other user, called party hangs up	PASS
2.5	Basic Calls	Outbound Call cancel	Call from Remote Worker and hang up before caller party answers	PASS
2.6	Basic Calls	Inbound Call cancel	Call to Remote Worker and disconnect the caller before call is established	PASS
2.7	Basic Calls	Outbound Hold/retrieve	Call from Remote Worker to other user, answers the call, caller puts call on hold, then retrieves the call	PASS
2.8	Basic Calls	Inbound hold/retrieve	Inbound call to Remote Worker, put the call at caller party after call is established, retrieve the call to ensure speech path is returned	PASS
2.9	Basic Calls	Outbound long duration	Call from Remote Worker phone to other device; Keep the call active for more than 30 minutes	PASS
2.10	Basic Calls	Inbound long duration	Call to Remote Worker and keep the call active for more than 30 minutes	PASS
3.1	Features	Unattended transfer	Call to Remote Worker; Unattended transfer to another user	PASS

3.2	Features	Unattended transfer	Remote Worker call User A; Unattended transfer to User B	PASS
3.3	Features	Consultative transfer	Remote Worker calls User A and transfers the call to User B	PASS
3.4	Features	Consultative transfer	User A calls Remote Worker and transfers to User B	PASS
3.5	Features	Call Forward All	Call Forward All is set on Remote Worker	PASS
3.6	Features	Call Forward Busy	Call Forward Busy is set on Remote Worker	PASS
3.7	Features	Call Forward No answer	Call Forward No Answer is set on Remote Worker	PASS
3.8	Features	Conference	Conference is made on Remote Worker	PASS
3.9	Features	Conference	Conference is made on Remote Worker	PASS
3.10	Features	Call Park/Retrieve	Call to Remote Worker, Remote Worker parks the call, call is retrieved by other user	PASS
3.11	Features	Call Pickup	Configure Remote Worker and User A in same Call Pickup group; Assign call pickup button on each phone	PASS
3.12	Features	Bridged Call Appearance	Configure Avaya system and phones with Bridged Call Appearance	PASS
3.13	Features	Voicemail Indicator on	Call to Remote Worker, forward to voicemail and leave message, MWI is on	PASS
3.14	Features	Voicemail Indicator off	Retrieve the message for Remote Worker and make sure the MWI on the phone turns off	PASS
3.15	Features	Voicemail	Remote Worker calls Voicemail and retrieves the voicemail, navigates the voicemail menu	PASS
3.16	Features	Share Control	Set Remote Worker in shared control mode	PASS
3.17	Features	Video	Video capable call from Remote Worker to another device	PASS
3.18	Features	Video	Video capable call from other user to Remote Worker	PASS
3.19	Features	Session Manager HA	Shutdown the primary Session Manager, check the phone registered to secondary SM	PASS
4.1	Presence/IM	Presence	Remote Worker phone displays presence status of other user	PASS
4.2	Presence/IM	Presence	Remote Worker presence status updates on other user's phone	PASS

5.1	TCP	Register / Keep Alive	Setup TCP among Oracle SBC, Avaya SIP devices and Session Manager	PASS
5.2	TCP	Outbound call	Call from Remote Worker to other users, caller hangs up after call is established	PASS
5.3	TCP	Inbound call	Call to Remote Worker from other user, calling party hangs up	PASS
6.1	NAT	Register / Keep Alive	Register One-X communicator to Avaya Session manager via Oracle SBC	PASS
6.2	NAT	Outbound call	Call from Remote Worker to other users, caller hangs up after call	PASS
6.3	NAT	Outbound Hold/retrieve	Call from Remote Worker to other user, answers the call, caller puts call on hold, then retrieves the call	PASS
6.4	NAT	Consultative transfer	User A calls Remote Worker and transfers to User B	PASS
6.5	NAT	Conference	Conference is made on Remote Worker	PASS

Avaya 7.0 Test Plan

External ID	External Test Case Type	Title	Description	Status (Pass or Fail etc)
1.1	General	Register / Keep Alive	Register Avaya SIP desktop phone to Avaya Session manager via Oracle SBC	PASS
1.2	General	Register / Keep Alive	Register One-X communicator to Avaya Session manager via Oracle SBC	PASS
1.3	General	Register / Keep Alive	Register One-X Mobile SIP (for IOS or Android) to Avaya Session manager via Oracle SBC	PASS
2.1	Basic Calls	Outbound call	Call from Remote Worker to other users, caller hangs up after call	PASS
2.2	Basic Calls	Outbound call	Call from Remote Worker to other users, called party hangs up after call	PASS
2.3	Basic Calls	Inbound call	Call to Remote Worker from other user, calling party hangs up	PASS
2.4	Basic Calls	Inbound call	Call to Remote Worker from other user, called party hangs up	PASS
2.5	Basic Calls	Outbound Call cancel	Call from Remote Worker and hang up before caller party answers	PASS
2.6	Basic Calls	Inbound Call cancel	Call to Remote Worker and disconnect the caller before call is established	PASS

2.7	Basic Calls	Outbound Hold/retrieve	Call from Remote Worker to other user, answers the call, caller puts call on hold, then retrieves the call	PASS
2.8	Basic Calls	Inbound hold/retrieve	Inbound call to Remote Worker, put the call at caller party after call is established, retrieve the call to ensure speech path is returned	PASS
2.9	Basic Calls	Outbound long duration	Call from Remote Worker phone to other device; Keep the call active for more than 30 minutes	PASS
2.10	Basic Calls	Inbound long duration	Call to Remote Worker and keep the call active for more than 30 minutes	PASS
3.1	Features	Unattended transfer	Call to Remote Worker; Unattended transfer to another user	PASS
3.2	Features	Unattended transfer	Remote Worker call User A; Unattended transfer to User B	PASS
3.3	Features	Consultative transfer	Remote Worker calls User A and transfers the call to User B	PASS
3.4	Features	Consultative transfer	User A calls Remote Worker and transfers to User B	PASS
3.5	Features	Call Forward All	Call Forward All is set on Remote Worker	PASS
3.6	Features	Call Forward Busy	Call Forward Busy is set on Remote Worker	PASS
3.7	Features	Call Forward No answer	Call Forward No Answer is set on Remote Worker	PASS
3.8	Features	Conference	Conference is made on Remote Worker	PASS
3.9	Features	Conference	Conference is made on Remote Worker	PASS
3.10	Features	Call Park/Retrieve	Call to Remote Worker, Remote Worker parks the call, call is retrieved by other user	PASS
3.11	Features	Call Pickup	Configure Remote Worker and User A in same Call Pickup group; Assign call pickup button on each phone	PASS
3.12	Features	Bridged Call Appearance	Configure Avaya system and phones with Bridged Call Appearance	PASS
3.13	Features	Voicemail Indicator on	Call to Remote Worker, forward to voicemail and leave message, MWI is on	PASS
3.14	Features	Voicemail Indicator off	Retrieve the message for Remote Worker and make sure the MWI on the phone turns off	PASS

3.15	Features	Voicemail	Remote Worker calls Voicemail and retrieves the voicemail, navigates the voicemail menu	PASS
3.16	Features	Share Control	Set Remote Worker in shared control mode	PASS
3.17	Features	Video	Video capable call from Remote Worker to another device	PASS
3.18	Features	Video	Video capable call from other user to Remote Worker	PASS
4.1	Presence/IM	Presence	Remote Worker phone displays presence status of other user	PASS
4.2	Presence/IM	Presence	Remote Worker presence status updates on other user's phone	PASS
5.1	NAT	Register / Keep Alive	Register One-X communicator to Avaya Session manager via Oracle SBC	PASS
5.2	NAT	Outbound call	Call from Remote Worker to other users, caller hangs up after call	PASS
5.3	NAT	Outbound Hold/retrieve	Call from Remote Worker to other user, answers the call, caller puts call on hold, then retrieves the call	PASS
5.4	NAT	Consultative transfer	User A calls Remote Worker and transfers to User B	PASS
5.5	NAT	Conference	Conference is made on Remote Worker	PASS

Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for Windows, Macs, Linux and the Oracle E-SBC and EOM like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

Wireshark

Wireshark is a network protocol analyzer which is freely downloadable from www.wireshark.org. Note that Wireshark traces taken directly from the network will show encrypted SIP/TLS, which can be useful for troubleshooting TLS issues but not necessarily SIP signaling issues.

On the Oracle E-SBC

The Oracle SBC provides a rich set of statistical counters available from the CLI, 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 console:

```
oraclesbc1# reset sipd
oraclesbc1# notify sipd debug
oraclesbc1#
enabled SIP Debugging
oraclesbc1# notify all rotate-logs
```

Examining the log files

Note: You will FTP to the management interface of the SBC 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 oraclesbc1FTP 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 /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (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.

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle E-SBC, and it provides traces in a common log format for local viewing or for exporting to your PC. Please check the "Monitor and Trace SIP Messages" section (page 140) of the E-SBC Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm.

Oracle Enterprise Operations Monitor (EOM)

The Oracle Enterprise Operations Monitor (EOM) can be used to analyze SIP signaling messages. See the example report at the end of the "Configuring EOM to Display All Legs of a Call in a Single Report" section above.

Appendix A

Accessing the ACLI

Access to the ACLI is provided by:

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

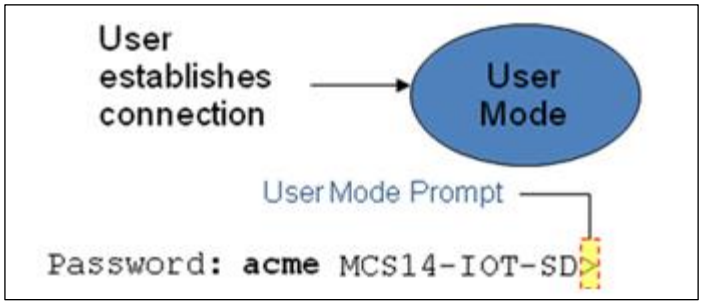
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

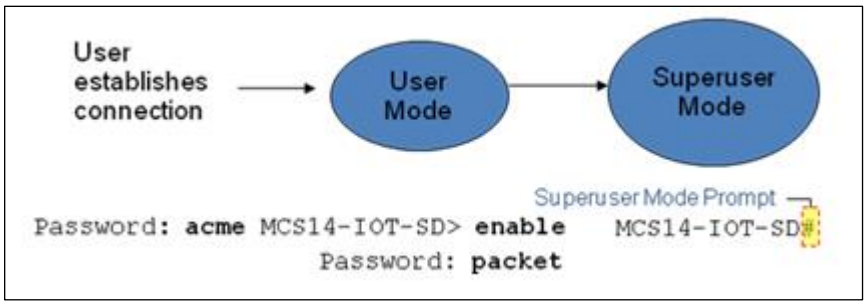
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the SBC, 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.



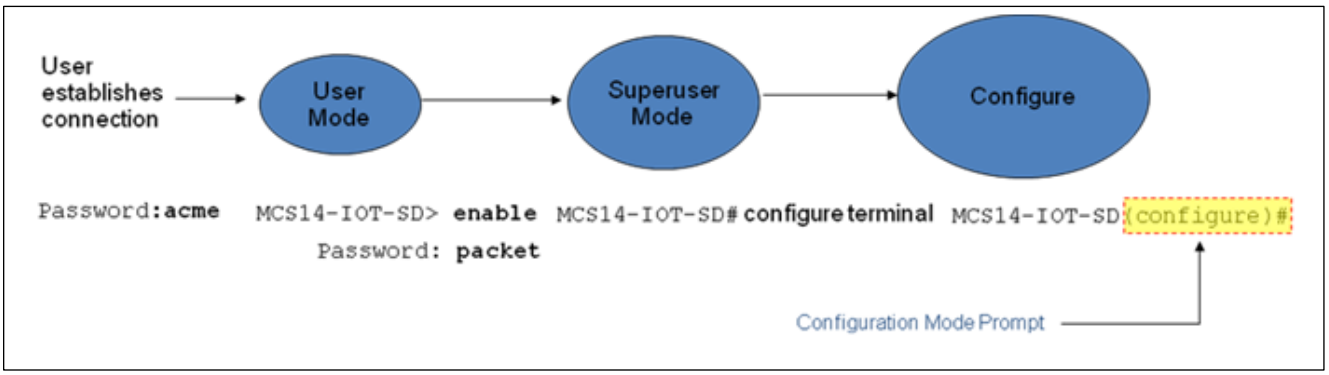
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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.

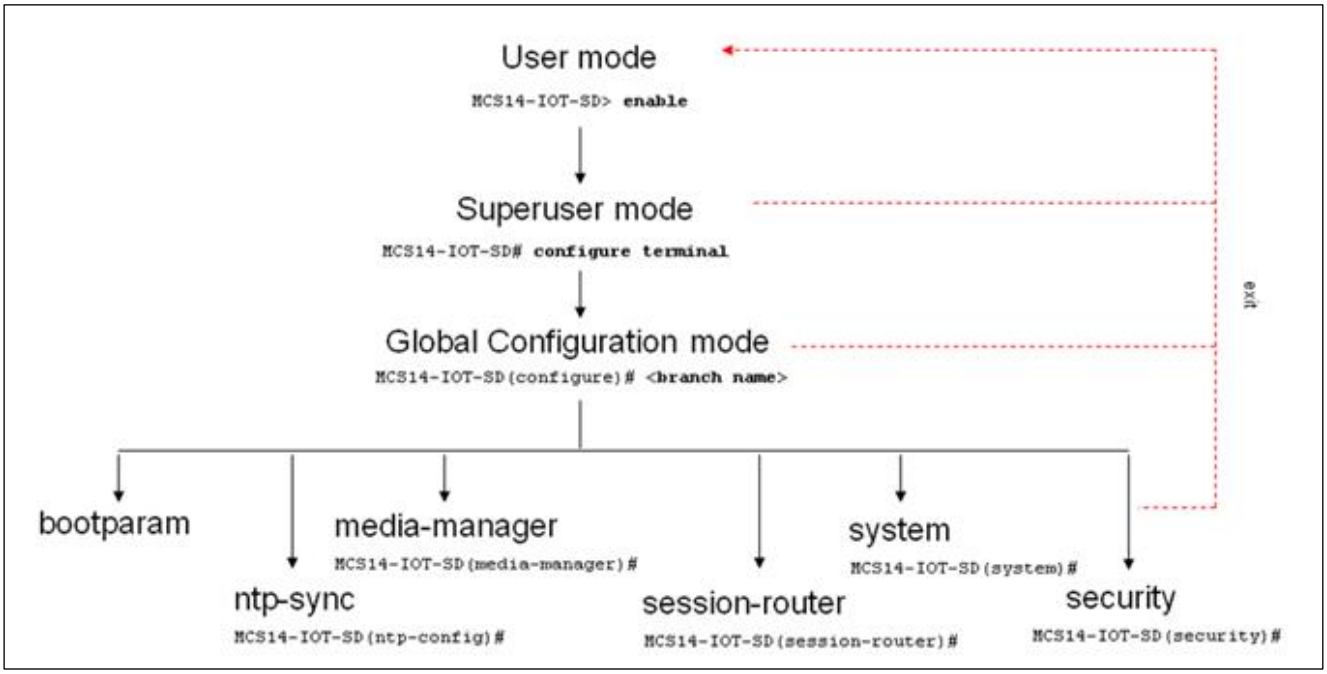
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **oraclesbc1(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.



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 SBC boot parameters.

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

The security branch provides access to security configuration.

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

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media-manager, and so forth.

You will use media-manager, 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:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

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 SBC 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 SBC 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 SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the SBC: 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 SBC'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 SBC 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 SBC displays a reminder on screen stating that you must use the **`activate-config`** command if you want the configurations to be updated.

```
oraclesbc1 # 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'.
oraclesbc1 #
```

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 SBC 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.

```
oraclesbc1# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1#
```


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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services