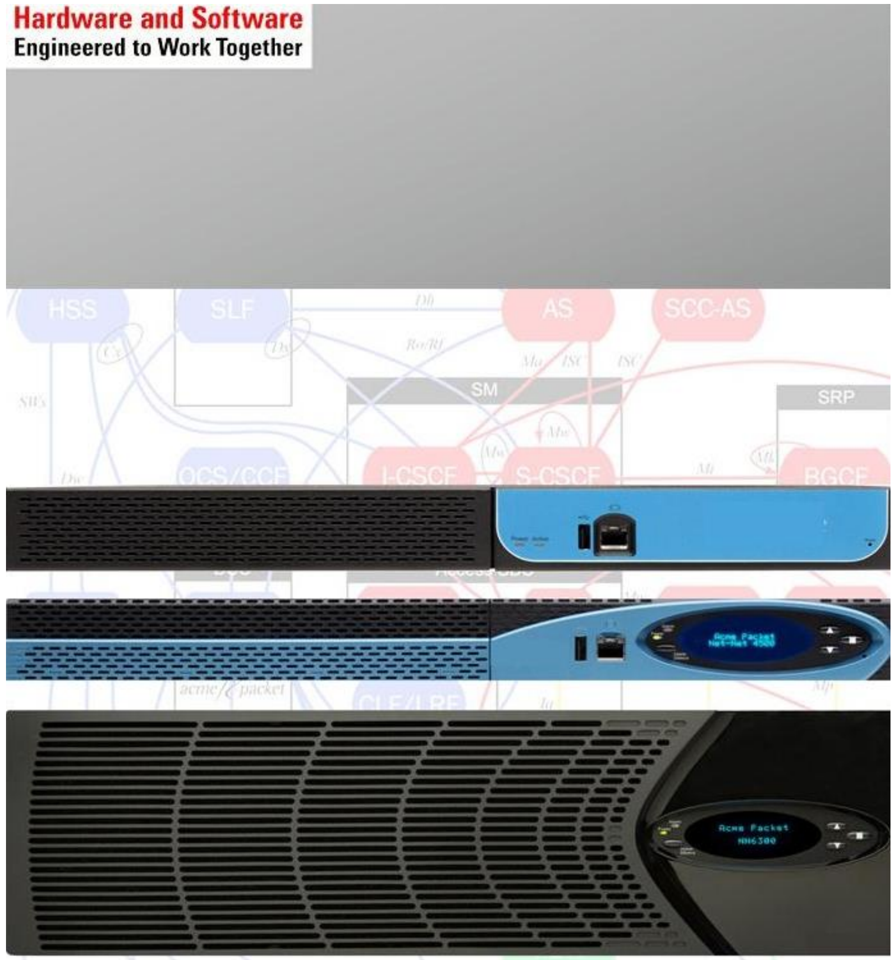


Oracle Enterprise Session Border Controller ECX6.4.0 with Verint Recorder 11.2 using Avaya Aura 6.0 and Cisco communication manager 9.0.

Technical Application Note

Disclaimer

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

Table of Contents

Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC). It assumes that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller.

Document Overview

This document is intended for use as a guide for a successful integration of both Verint Recorder and Oracle Enterprise Session Border Controller. It outlines the architecture design, E-SBC configuration including troubleshooting tools, as well as test cases executed as part of the interoperability testing.

Introduction

Audience

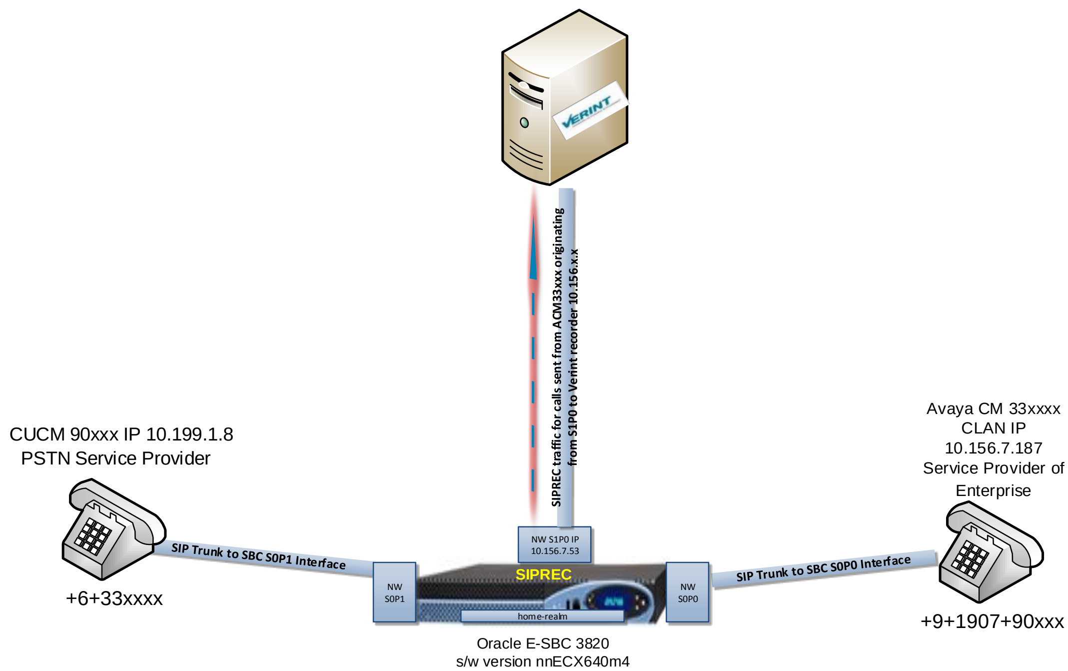
This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller and the changes to be done in Verint Recorder, Avaya CM and CUCM for this interop testing. Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Requirements

- Acme Packet 3800 with Firmware Release ECX6.4.0 MR-4 GA (Build 413)
- Avaya CM Software Version 6.02.0.823.0
- Cisco UCM Software Version 9.0.1.10000-37
- Avaya IP phone type 4625
- Avaya One-X IP phone type 9620/9630
- Cisco IP Communicator softphone
- Cisco IP phone type 7940
- Verint recorder – Release 11.2

Architecture

The following reference architecture shows a logical view of the connectivity between Avaya, Cisco and Verint elements and the E-SBC.



The network diagram demonstrates that the E-SBC is connected as an edge component for the Avaya Session Manager and Cisco Call Manager. The E-SBC connects Enterprise to Enterprise via a SIP trunk, and the Verint recorder can be located on either domain, but is located on a separate domain for this testing. The E-SBC supports the SIPREC standard which is used for recording the call and sending the recorded stream to the Verint recorders. The SIPREC protocol is used to interact between a Session Recording Client (SRC - the role performed by E-SBC) and a Session Recording Server (SRS- Verint recorder).

Configuring the Oracle Enterprise Session Border Controller (E-SBC)

In this section we describe the steps for configuring an E-SBC, formally known as the Acme Packet Net-Net Enterprise Session Director for use with Avaya CM, CUCM and Verint recorder in a SIP trunking scenario.

In Scope

The following step-by-step guide configuring the E-SBC assumes that this is a newly deployed device dedicated to a single customer.

Note that Oracle offers several models of SBCs. This document covers the setup for the Acme Packet 3820 and 4500 platform series running ECX 6.4.0m4 or later. If instructions are needed for other Oracle E-SBC models, please contact your Oracle representative.

Out of Scope

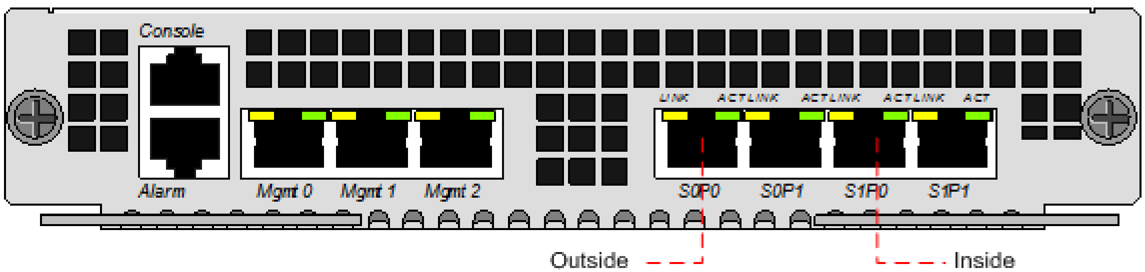
- Configuration of Network management including SNMP and RADIUS; and
- Redundancy configuration
- Complete configuration of the Avaya Call Manager, Cisco UCM and the Verint recorder.

What will you need

- Serial Console cross over cable with RJ-45 connector
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle E-SBC
- IP address to be assigned to management interface (Wancom0) of the E-SBC - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the E-SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support E-SBC configurations with management and media/service interfaces on the same subnet.
- IP address of the Avaya CM, CUCM and Verint Recorder
- IP address to be used for the E-SBC internal and external facing ports (Service Interfaces)

Configuring the E-SBC

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



Plug the slot 0 port 0 (s0p0) interface into your Avaya facing gateway and the slot 0 port 1 (s0p1) interface into Cisco facing gateway. The slot 1 port 0 (s1p0) is connected to the Verint recorder. Once connected, you are ready to power on and perform the following steps.

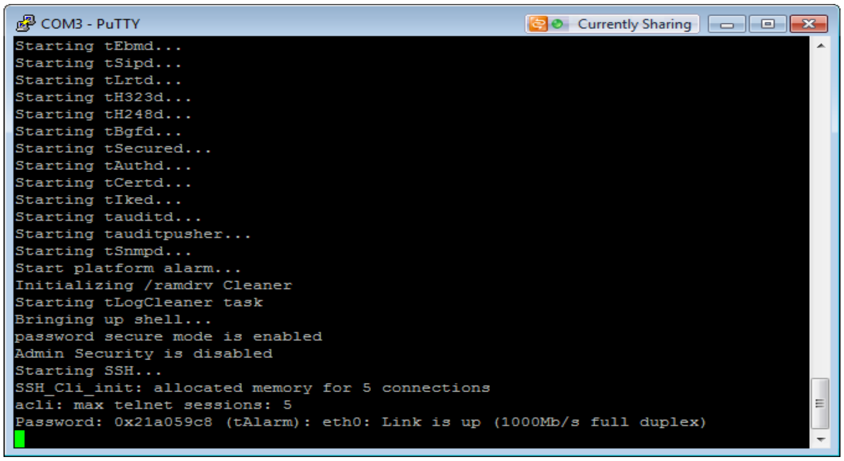
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as ACMESYSTEM are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the E-SBC

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

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

Power on the E-SBC and confirm that you see the following output from the bootup sequence.



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

```
Password: acme
ACMESYSTEM> enable
Password: packet
ACMESYSTEM# configure terminal
ACMESYSTEM(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 E-SBC by going to

ACMESYSTEM# configure terminal --- >bootparams

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

```
ACMESYSTEM#(configure)bootparam
'.' = clear field;  '-' = go to previous field;  q = quit
boot device              : eth0
processor number         : 0
host name                : acmesystem
file name                : /code/images/nnECX640m2.tar--- >location where
the software is loaded on the SBC
inet on ethernet (e)     : 172.18.255.52:ffffff80 --- > This is the ip
address of the management interface of the SBC, type the IP address and
mask in hex
inet on backplane (b)    :
host inet (h)            :
gateway inet (g)         : 172.18.0.1 --- > gateway address here
user (u)                 : vxftp
ftp password (pw) (blank = use rsh)     : vxftp
flags (f)                :
target name (tn)         : ACMESYSTEM
startup script (s)       :
other (o)                :
```

Configuring the E-SBC

The following section walks you through configuring the Oracle Enterprise Session Border Controller to work with the Avaya CM, Cisco CM and the Verint recorders.

The calls are recorded by a Verint recorder which is added to the configuration using session-recording-server and session-recording-group. The session recorders are defined in the session-recording-group, and the session-recording-group is referenced from the realm-config. In our case, the session-recording-group has three session recording servers SRS1, SRS2 and SRS3 which are defined in the group using Hunt strategy. Also, since we need all the calls to be simultaneously recorded, simultaneous-recording-servers is defined as 3. The session-recording-server element has details of the session recorder such as the IP and port, as also the realm to which it belongs. Another field with reference to call recording in the realm-config is the session-recording-required. If session-recording-required =enabled, then the calls between the two parties will not go through unless the session recorder is ready and available to record.

Also, as often in contact center applications, a unique ID is needed to co-relate the recorded calls, an Avaya UCID is used for this purpose in this testing. The Universal Call Identifier SPL plug-in generates or preserves a UCID based on configuration. Once a UCID is generated or preserved, the system adds the value to all subsequent egress SIP requests within the session. This SPL plugin is already present in /modules in the ECX640m4 image, so it need not be explicitly loaded on the E-SBC, but you do need to enable the plugin with the SPL option UCID-App-ID=0024 in the spl-config element. The UCID-App-ID SPL option allows the E-SBC to examine ingress SIP requests for the “User-to-User” header. When present, the header is transparently passed through the egress SIP message. If set to replace-ucid or the header is not present, the system generates a new value for “User-to-User”.

You must set the value to a 2-byte hex-ascii value that represents the app ID which is the identifying value, as defined by the vendors. All input is truncated to 4 characters. Any characters outside the range of 0-9 and A-F will result in an invalid User-to-User header. The UCID is added as an extension data to the session element of the recording's metadata when using SIPREC.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment. Following is the configuration with which the testing has taken place:

```
host-routes
        dest-network                            10.0.0.0
        netmask                                 255.0.0.0
        gateway                                 10.156.0.254
        description
        last-modified-by                        admin@console
        last-modified-date                      2014-02-02 12:30:02
local-policy
        from-address                            *
        to-address                              *
        source-realm                            ACM33xxxxATL_realm
        description                             local_policy_Avaya33xxxx
        activate-time
        deactivate-time
        state                                   enabled
        policy-priority                         none
        policy-attribute
                next-hop                                10.199.1.8
                realm                                   CUCM90xxxATL_realm
                action                                  none
                terminate-recursion                     disabled
                carrier
                start-time                              0000
                end-time                                2400
                days-of-week                            U-S
                cost                                    0
                state                                   enabled
                app-protocol                            SIP
                methods
                media-profiles
                lookup                                  single
                next-key
                eloc-str-lkup                           disabled
                eloc-str-match
```

```
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-03-23 05:44:00
local-policy
        from-address                            *
        to-address                              33
        source-realm                            CUCM90xxxATL_realm
        description                             local_policy_Cisco90xxx
        activate-time
        deactivate-time
        state                                   enabled
        policy-priority                         none
        policy-attribute
                next-hop                                10.156.7.187
                realm                                   ACM33xxxxATL_realm
                action                                  none
                terminate-recursion                     disabled
                carrier
                start-time                              0000
                end-time                                2400
                days-of-week                            U-S
                cost                                    0
                state                                   enabled
                app-protocol                            SIP
                methods
                media-profiles
                lookup                                  single
                next-key
                eloc-str-lkup                           disabled
                eloc-str-match
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-05-04 07:42:06
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
        app-signaling-bandwidth                 0
        tolerance-window                        30
        trap-on-demote-to-deny                  disabled
        syslog-on-demote-to-deny                disabled
        syslog-on-demote-to-untrusted           disabled
        rtcp-rate-limit                         0
        anonymous-sdp                           disabled
        arp-msg-bandwidth                       32000
        fragment-msg-bandwidth                  0
        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
        last-modified-by                        admin@console
        last-modified-date                      2013-12-17 12:03:00
network-interface
        name                                    S0P0
        sub-port-id                             0
        description                             Avaya_Traffic
        hostname
        ip-address                              10.156.9.1
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.0.0
        gateway                                 10.156.0.254
        sec-gateway
```

```
        gw-heartbeat
                state                                       enabled
                heartbeat                                   0
                retry-count                                 0
                retry-timeout                               1
                health-score                                0
        dns-ip-primary                              10.156.2.8
        dns-ip-backup1                              10.156.2.10
        dns-ip-backup2
        dns-domain                                  lab.local
        dns-timeout                                 11
        hip-ip-list                                 10.156.7.60
                                                    10.156.7.61
                                                    10.156.9.1
        ftp-address                                 10.156.7.61
        icmp-address                                10.156.7.60
                                                    10.156.7.61
                                                    10.156.9.1
        snmp-address
        telnet-address                              10.156.7.60
        ssh-address                                 10.156.7.61
        last-modified-by                            admin@10.56.20.14
        last-modified-date                          2014-07-29 15:18:02
network-interface
        name                                        S0P1
        sub-port-id                                 0
        description                                 Cisco_Traffic
        hostname
        ip-address                                  10.156.7.51
        pri-utility-addr
        sec-utility-addr
        netmask                                     255.255.0.0
        gateway                                     10.156.0.254
        sec-gateway
        gw-heartbeat
                state                                       enabled
                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
        hip-ip-list                             10.156.7.51
        ftp-address
        icmp-address                            10.156.7.51
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                        admin@console
        last-modified-date                      2014-02-02 11:38:32
network-interface
        name                                    S1P0
        sub-port-id                             0
        description                             recorder_network_S1P0
        hostname
        ip-address                              10.156.7.53
        pri-utility-addr
        sec-utility-addr
        netmask                                 255.255.0.0
        gateway                                 10.156.0.254
        sec-gateway
        gw-heartbeat
                state                                   enabled
                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
        hip-ip-list                             10.156.7.53
        ftp-address
        icmp-address                            10.156.7.53
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                        admin@console
```

```
        last-modified-date                     2014-02-02 11:55:02
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
        last-modified-by                       admin@10.61.20.68
        last-modified-date                     2014-03-23 05:47:21
phy-interface
        name                                   S0P1
        operation-type                         Media
        port                                   1
        slot                                   0
        virtual-mac
        admin-state                            enabled
        auto-negotiation                       enabled
        duplex-mode                            FULL
        speed                                  100
        wancom-health-score                    50
        overload-protection                    disabled
        last-modified-by                       admin@console
        last-modified-date                     2013-12-18 11:04:45
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
```

```
        last-modified-by                        admin@console
        last-modified-date                      2014-02-02 11:25:36
realm-config
        identifier                              ACM33xxxxATL_realm
        description                             AvayaCC33xxxx
        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
        generate-UDP-checksum                   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                      ACME_NAT_TO_FROM_IP
        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
        deny-period                             30
        cac-failure-threshold                   0
        untrust-cac-failure-threshold           0
        ext-policy-svr
```

```
        diam-e2-address-realm
        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
        refer-notify-provisional                none
        dyn-refer-term                          disabled
        codec-policy
        codec-manip-in-realm                    disabled
        constraint-name
        call-recording-server-id
        session-recording-server                SRG:SBC_TLV_SRG
        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
        monitoring-filters
        last-modified-by                            admin@10.61.20.68
        last-modified-date                          2014-05-12 08:28:23
realm-config
        identifier                                  CUCM90xxxATL_realm
        description                                 Cisco90xxxPSTN
        addr-prefix                                 0.0.0.0
        network-interfaces                          S0P1:0
        mm-in-realm                                 disabled
        mm-in-network                               enabled
        mm-same-ip                                  enabled
        mm-in-system                                enabled
        bw-cac-non-mm                               disabled
        msm-release                                 disabled
        generate-UDP-checksum                       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                          ACME_NAT_TO_FROM_IP
        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
```

```
deny-period                             30
cac-failure-threshold                   0
untrust-cac-failure-threshold           0
ext-policy-svr
diam-e2-address-realm
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
refer-notify-provisional                none
dyn-refer-term                          disabled
codec-policy
codec-manip-in-realm                    disabled
constraint-name
call-recording-server-id
session-recording-server
session-recording-required              disabled
manipulation-string
manipulation-pattern
stun-enable                             disabled
stun-server-ip                          0.0.0.0
stun-server-port                        3478
stun-changed-ip                         0.0.0.0
```

```
        stun-changed-port                               3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                                      disabled
        hide-egress-media-update                        disabled
        monitoring-filters
        last-modified-by                                admin@console
        last-modified-date                              2014-02-02 12:21:32
realm-config
        identifier                                      Recorder_realm
        description                                     Verint_Recorder
        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
        generate-UDP-checksum                           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
deny-period                           30
cac-failure-threshold                 0
untrust-cac-failure-threshold         0
ext-policy-svr
diam-e2-address-realm
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
refer-notify-provisional              none
dyn-refer-term                        disabled
codec-policy
codec-manip-in-realm                  disabled
constraint-name
call-recording-server-id
session-recording-server
session-recording-required            disabled
manipulation-string
manipulation-pattern
```

```
        stun-enable                                     disabled
        stun-server-ip                                  0.0.0.0
        stun-server-port                                3478
        stun-changed-ip                                 0.0.0.0
        stun-changed-port                               3479
        sip-profile
        sip-isup-profile
        match-media-profiles
        qos-constraint
        block-rtcp                                      disabled
        hide-egress-media-update                        disabled
        monitoring-filters
        last-modified-by                                admin@10.61.20.68
        last-modified-date                              2014-05-12 07:59:17
session-agent
        hostname                                        10.156.7.187
        ip-address                                      10.156.7.187
        port                                            5060
        state                                           enabled
        app-protocol                                    SIP
        app-type
        transport-method                                StaticTCP
        realm-id                                        ACM33xxxxATL_realm
        egress-realm-id
        description                                     Avaya33xxxxATL_c-lan08a13
        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
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                              UCID-App-ID=0024
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
```

```
        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
        send-tcp-fin                                   disabled
        last-modified-by                               admin@10.61.20.68
        last-modified-date                             2014-06-10 07:41:03
session-agent
        hostname                                       10.199.1.8
        ip-address                                     10.199.1.8
        port                                           5060
        state                                          enabled
        app-protocol                                   SIP
        app-type
        transport-method                               StaticTCP
        realm-id                                       CUCM90xxxATL_realm
        egress-realm-id
        description                                    Cisco90xxxATL_PSTN
        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
        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
```

```
        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
        send-tcp-fin                            disabled
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-05-12 08:22:11
session-recording-group
        name                                    SBC_TLV_SRG
        description                     session-recording-group-SIPREC-TLV
        strategy                                Hunt
        simultaneous-recording-servers          3
        session-recording-servers               SRS1
                                                SRS2
                                                SRS3
        last-modified-by                        admin@10.61.20.63
        last-modified-date                      2014-08-25 07:20:32
session-recording-server
        name                                    SRS1
        description                             ie-2k8rec-3
        realm                                   Recorder_realm
        mode                                    selective
        destination                             10.156.5.8
        port                                    5060
        transport-method                        StaticTCP
        ping-method                             OPTIONS
        ping-interval                           10
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-06-08 02:22:41
session-recording-server
        name                                    SRS2
        description                             ie-qa2k8-14
        realm                                   Recorder_realm
        mode                                    selective
```

```
        destination                                 10.156.13.218
        port                                        5060
        transport-method                            StaticTCP
        ping-method                                 OPTIONS
        ping-interval                               30
        last-modified-by                            admin@console
        last-modified-date                          2014-08-12 08:17:42
session-recording-server
        name                                        SRS3
        description                                 ie-qa2k12-4
        realm                                       Recorder_realm
        mode                                        selective
        destination                                 10.156.16.57
        port                                        5060
        transport-method                            StaticTCP
        ping-method                                 OPTIONS
        ping-interval                               10
        last-modified-by                            admin@10.61.20.63
        last-modified-date                          2014-09-18 02:17:22
sip-config
        state                                       enabled
        operation-mode                              dialog
        dialog-transparency                         enabled
        home-realm-id
        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
        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                                 sag-target-uri=ip
        add-reason-header                       disabled
        sip-message-len                         4096
        enum-sag-match                          disabled
        extra-method-stats                      disabled
        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
        pass-gruu-contact                       disabled
        sag-lookup-on-redirect                  disabled
        set-disconnect-time-on-bye              disabled
        last-modified-by                        admin@console
        last-modified-date                      2014-01-07 03:44:24
sip-interface
        state                                   enabled
        realm-id                                ACM33xxxxATL_realm
        description                             Avaya_Traffic
        sip-port
                address                                 10.156.9.1
                port                                    5060
                transport-protocol                      TCP
                tls-profile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        sip-port
                address                                 10.156.9.1
                port                                    5060
                transport-protocol                      UDP
                tls-profile
```

```
        allow-anonymous                         all
        multi-home-addrs
        ims-aka-profile
    carriers
    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
    out-manipulationid
    sip-ims-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
        ims-aka-feature                         disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        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
        session-recording-server
        session-recording-required              disabled
        service-tag
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-05-12 08:04:00
sip-interface
        state                                   enabled
        realm-id                                CUCM90xxxATL_realm
        description                             Cisco_Traffic
        sip-port
                address                                 10.156.7.51
                port                                    5060
                transport-protocol                      TCP
```

```
        tls-profile
        allow-anonymous                         all
        multi-home-addrs
        ims-aka-profile
    sip-port
        address                                 10.156.7.51
        port                                    5060
        transport-protocol                      UDP
        tls-profile
        allow-anonymous                         all
        multi-home-addrs
        ims-aka-profile
    carriers
    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
    out-manipulationid
```

```
sip-ims-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
ims-aka-feature                         disabled
enforcement-profile
route-unauthorized-calls
tcp-keepalive                           none
add-sdp-invite                          disabled
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
session-recording-server
session-recording-required              disabled
service-tag
last-modified-by                        admin@console
```

```
        last-modified-date                      2014-02-02 12:48:06
sip-interface
        state                                   enabled
        realm-id                                Recorder_realm
        description                             SIPREC_Traffic
        sip-port
                address                                 10.156.7.53
                port                                    5060
                transport-protocol                      TCP
                tls-profile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        sip-port
                address                                 10.156.7.53
                port                                    5060
                transport-protocol                      UDP
                tls-profile
                allow-anonymous                         all
                multi-home-addrs
                ims-aka-profile
        carriers
        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
        out-manipulationid
        sip-ims-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
        ims-aka-feature                         disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                           none
        add-sdp-invite                          disabled
        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
        session-recording-server
        session-recording-required              disabled
        service-tag
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-05-12 08:04:23
spl-config
        spl-options                             UCID-App-ID=0024
        last-modified-by                        admin@console
        last-modified-date                      2014-09-11 07:01:33
steering-pool
        ip-address                              10.156.7.51
        start-port                              49152
        end-port                                65535
        realm-id                                CUCM90xxxATL_realm
        network-interface
        last-modified-by                        admin@console
        last-modified-date                      2014-02-02 12:24:06
steering-pool
        ip-address                              10.156.7.53
        start-port                              49152
        end-port                                65535
        realm-id                                Recorder_realm
        network-interface
        last-modified-by                        admin@console
        last-modified-date                      2014-02-02 12:24:33
steering-pool
        ip-address                              10.156.9.1
        start-port                              49152
        end-port                                65535
        realm-id                                ACM33xxxxATL_realm
        network-interface
        last-modified-by                        admin@10.61.20.68
        last-modified-date                      2014-03-23 06:03:11
system-config
        hostname
        description
```

```
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                        enabled
        enable-snmp-auth-traps              disabled
        enable-snmp-syslog-notify           disabled
        enable-snmp-monitor-traps           disabled
        enable-env-monitor-traps            disabled
        snmp-syslog-his-table-length        1
        snmp-syslog-level                   WARNING
        system-log-level                    WARNING
        process-log-level                   WARNING
        process-log-ip-address              0.0.0.0
        process-log-port                    0
        collect
                sample-interval                     5
                push-interval                       15
                boot-state                          disabled
                start-time                          now
                end-time                            never
                red-collect-state                   disabled
                red-max-trans                       1000
                red-sync-start-time                 5000
                red-sync-comp-time                  1000
                push-success-trap-state             disabled
        comm-monitor
                state                               disabled
                sbc-grp-id                          0
                tls-profile
                qos-enable                          enabled
        call-trace                          disabled
        internal-trace                      disabled
        log-filter                          all
        default-gateway                     10.156.0.254
        restart                             enabled
        exceptions
        telnet-timeout                      0
        console-timeout                     0
        remote-control                      enabled
        cli-audit-trail                     enabled
```

```
        link-redundancy-state                  disabled
        source-routing                         disabled
        cli-more                               disabled
        terminal-height                        24
        debug-timeout                          0
        trap-event-lifetime                    0
        ids-syslog-facility                    -1
        options
        default-v6-gateway                     ::
        ipv6-signaling-mtu                     1500
        ipv4-signaling-mtu                     1500
        cleanup-time-of-day                    00:00
        snmp-engine-id-suffix
        snmp-agent-mode                        v1v2
        last-modified-by                       admin@10.61.20.68
        last-modified-date                     2014-03-26 10:43:27
```

Verify configuration integrity

You will verify your configuration referential integrity before saving and activating it with the verify-**config** command. This command is available from Superuser Mode. To enter the Superuser Mode from session-agent, you issue the **exit** command three times.

```
ACMESYSTEM# verify-config
----------------------------------------------------------------------

Verification successful! No errors nor warnings in the configuration
```

Save and activate your configuration

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.

```
ACMESYSTEM# 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'.

ACMESYSTEM# 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
```

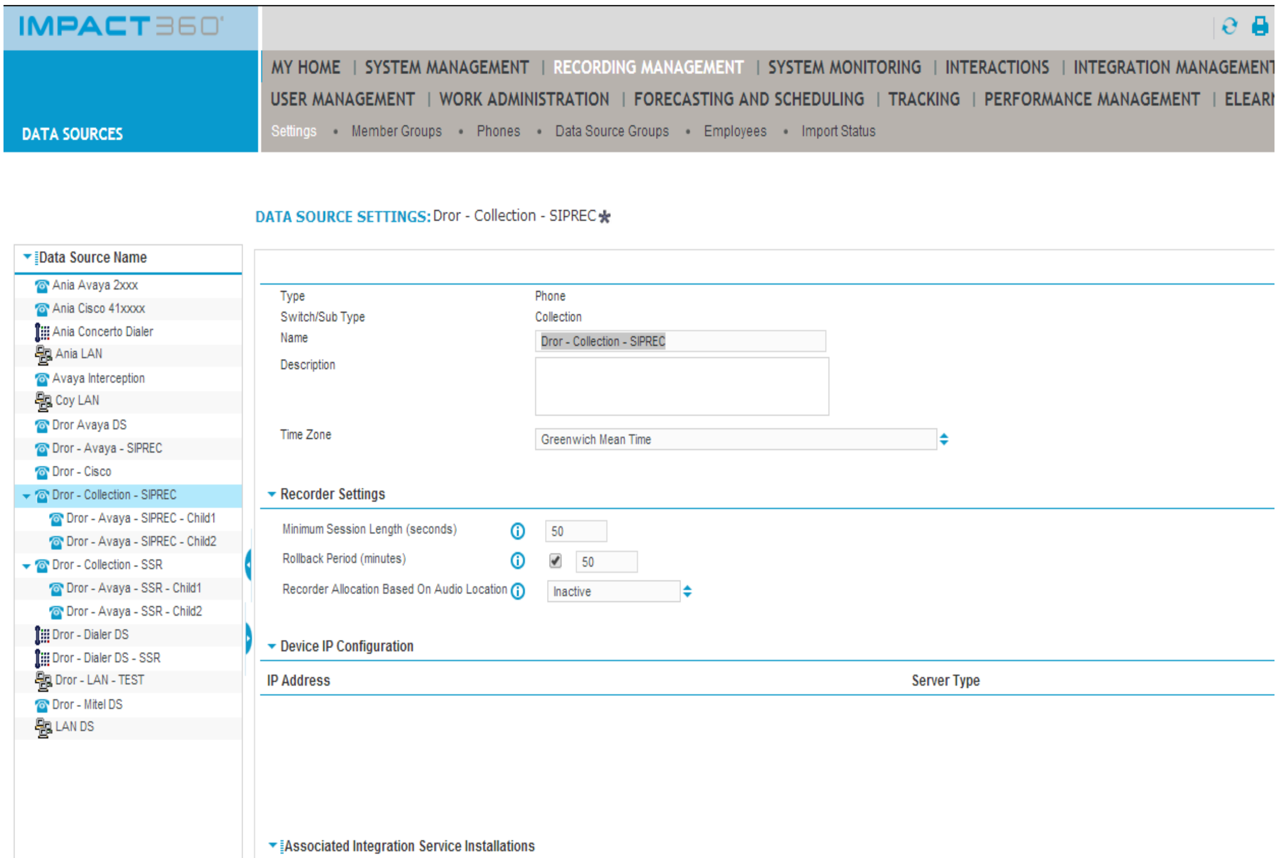
E-SBC configuration is now complete.

Verint Recorder Configuration changes

Step 1: Data Source Level

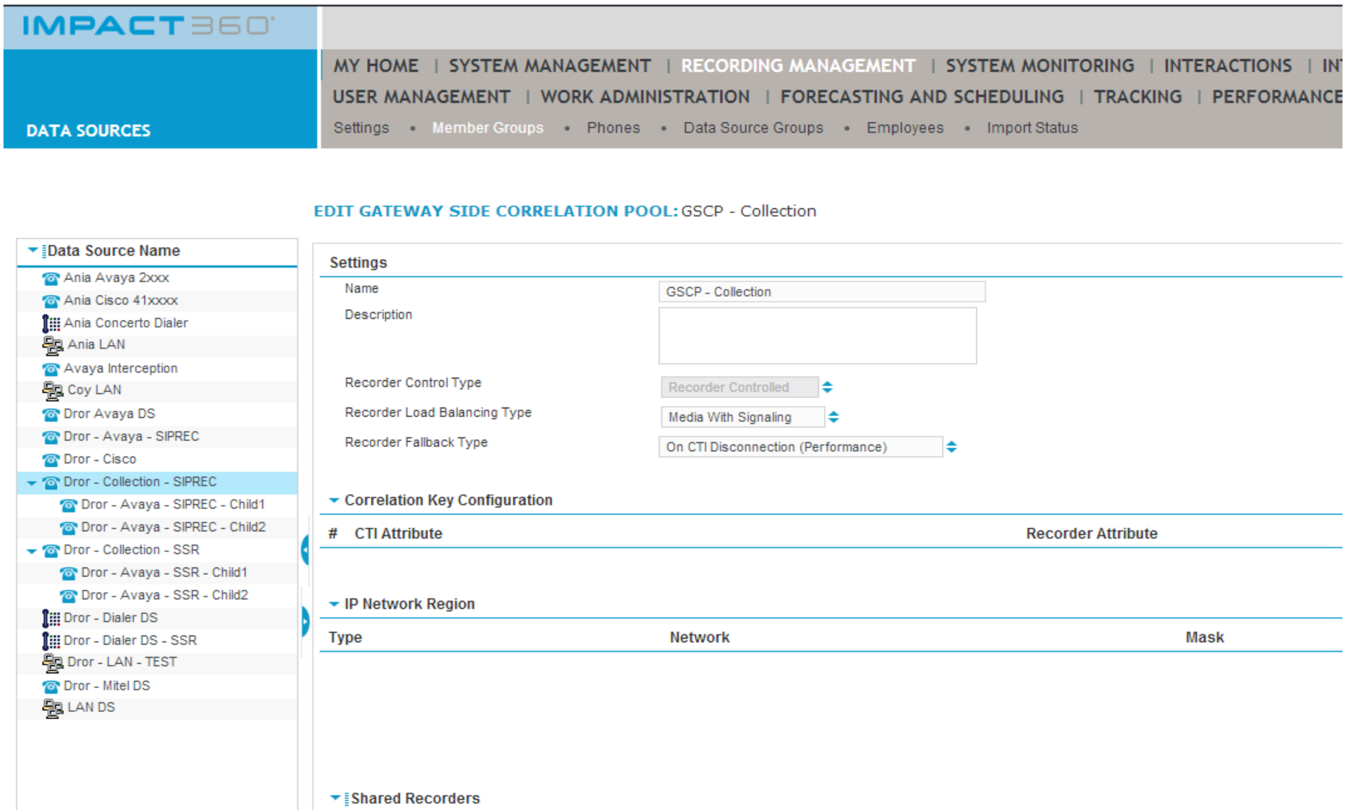
Insert your recorder to the Installation Tree with the following roles:

- Content Server
- IP Recorder
- Recorder Integration Service
- Screen Recorder



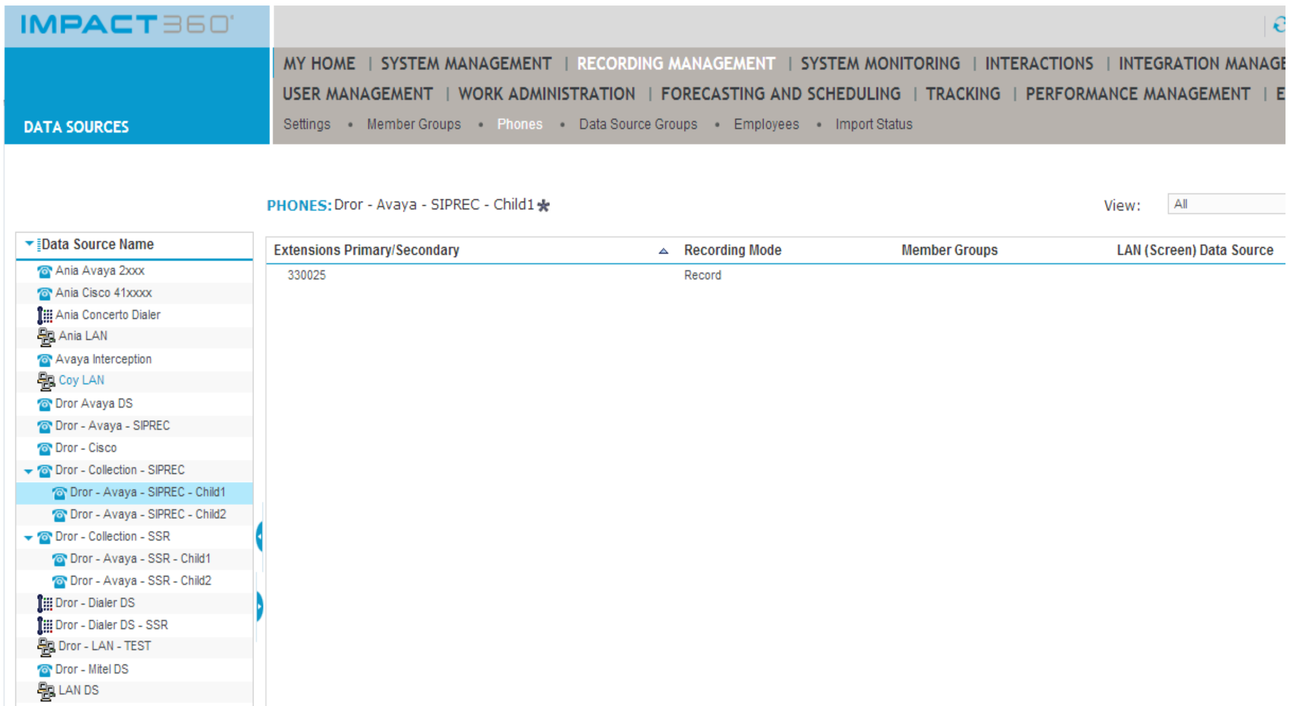
Step 2: Member Group Level

Create a Gateway Side Correlation Pool. Make sure that your IP Recorder role is on “Record”.



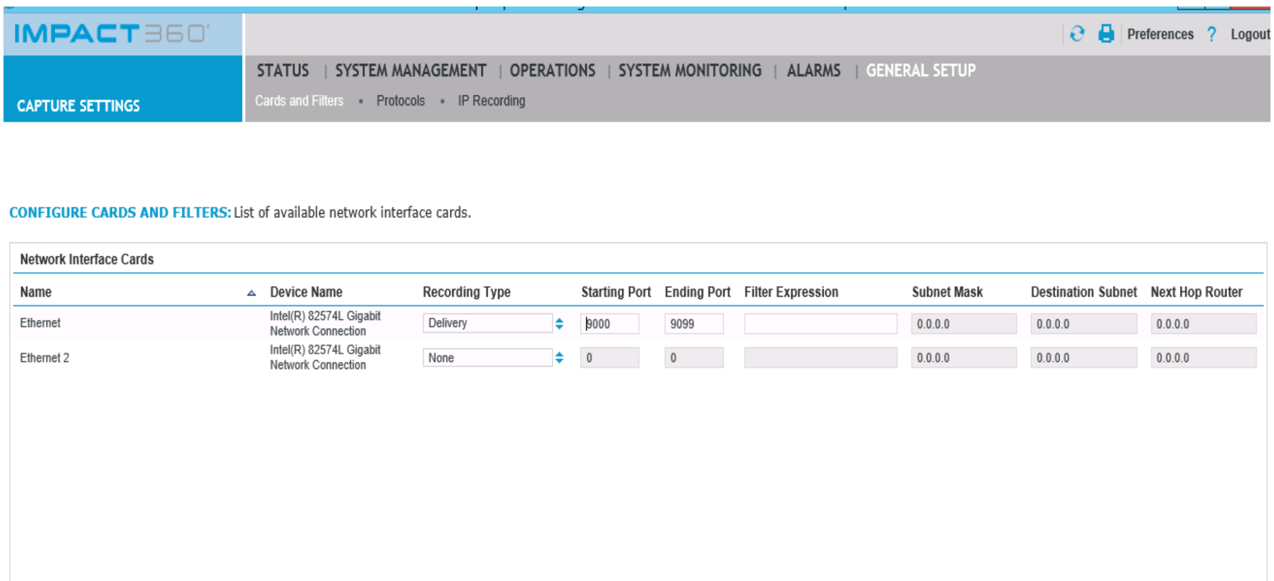
Step 3: Assign Member Group phones

Assign a dedicated Avaya IP phone; for example Line 330025. Associate you integration service to your IP Recorder and Screen Recorder.



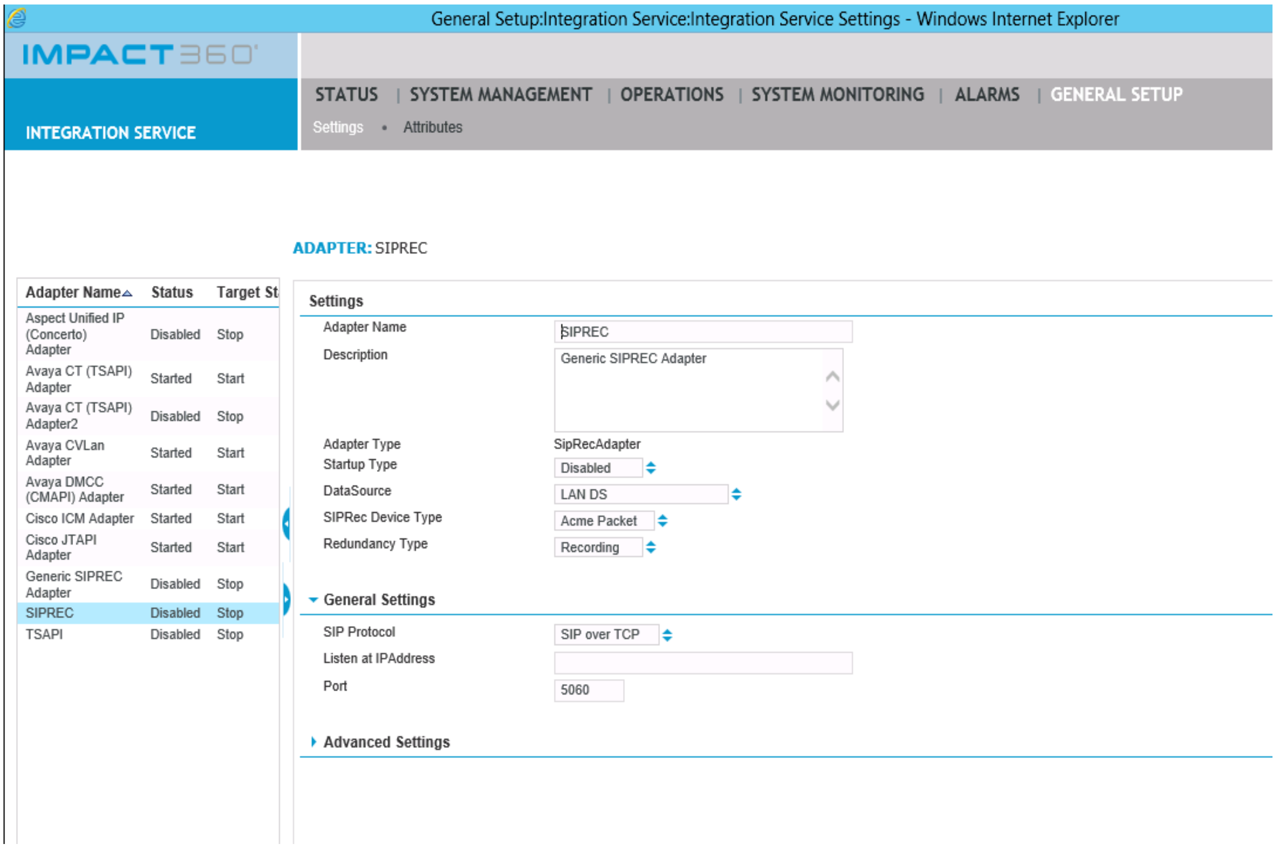
Step 4: Network Cards Level

Set dedicated network interface as ‘Delivery’. Associate you integration service to your IP Recorder and Screen Recorder.

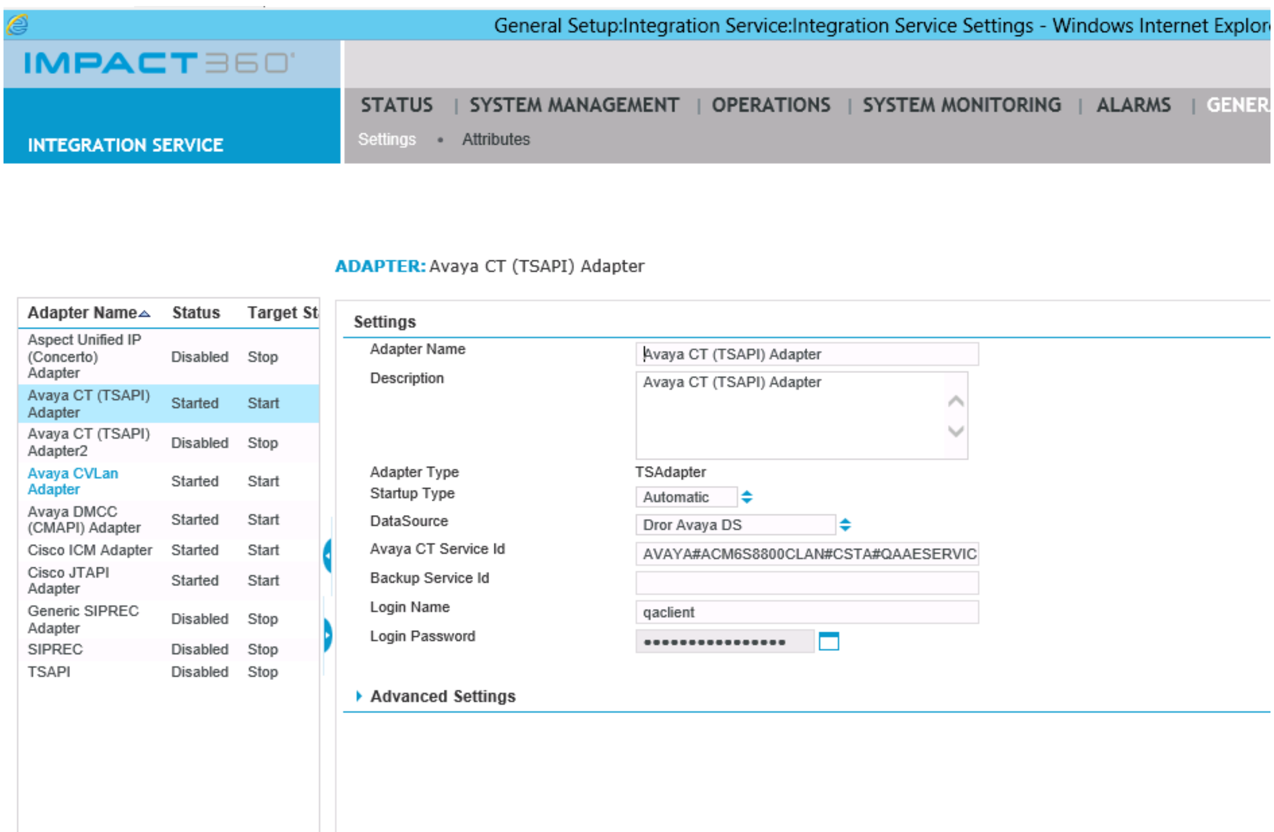


Step 5: Integration Service Settings

Select dedicated ‘SIPREC’ adapter. Associate you integration service to your IP Recorder and Screen Recorder.



Create a dedicated Avaya TSAPI adapter to connect to ACM33xxxx CTI link. Associate you integration service to your IP Recorder and Screen Recorder.



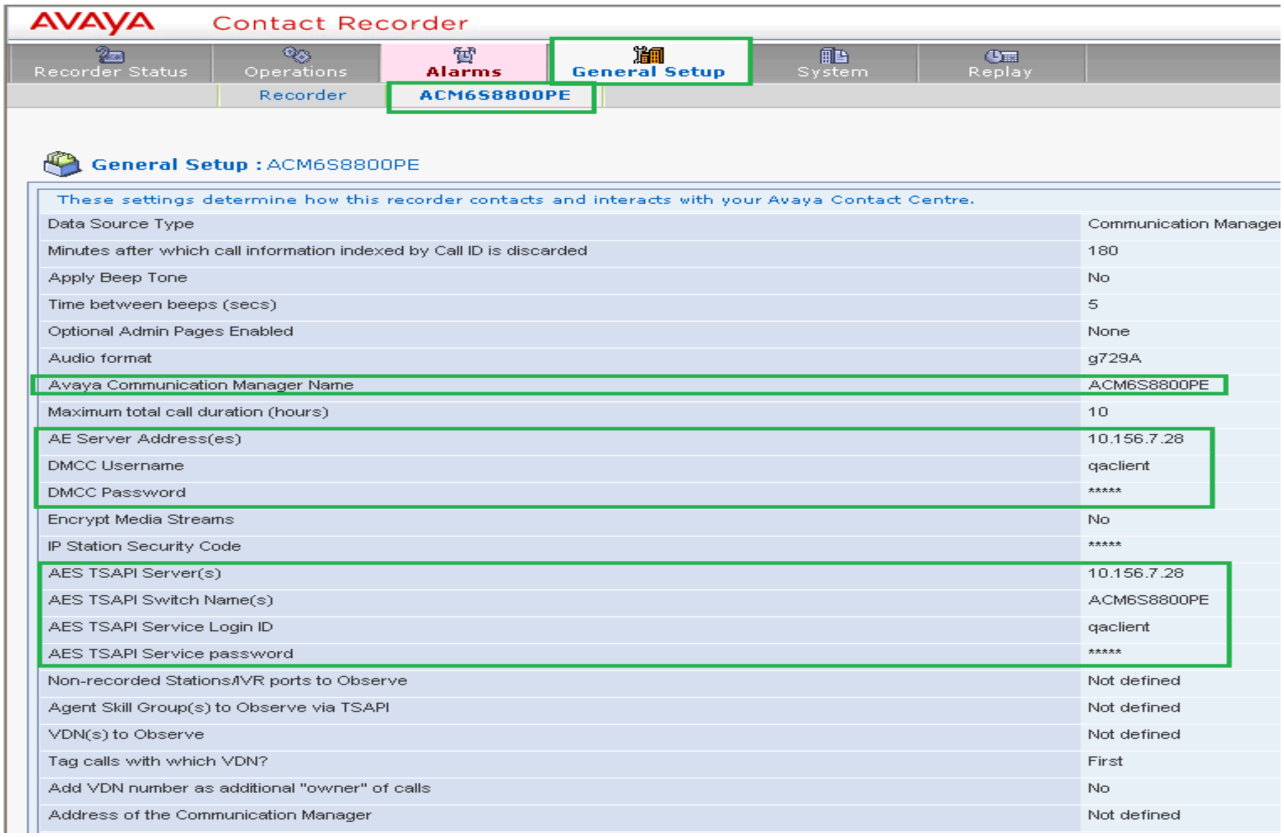
Avaya Contact Recording Setup

Step1: Integration Service Settings

Create a dedicated Avaya TSAPI adapter to connect to ACM33xxxx CTI link

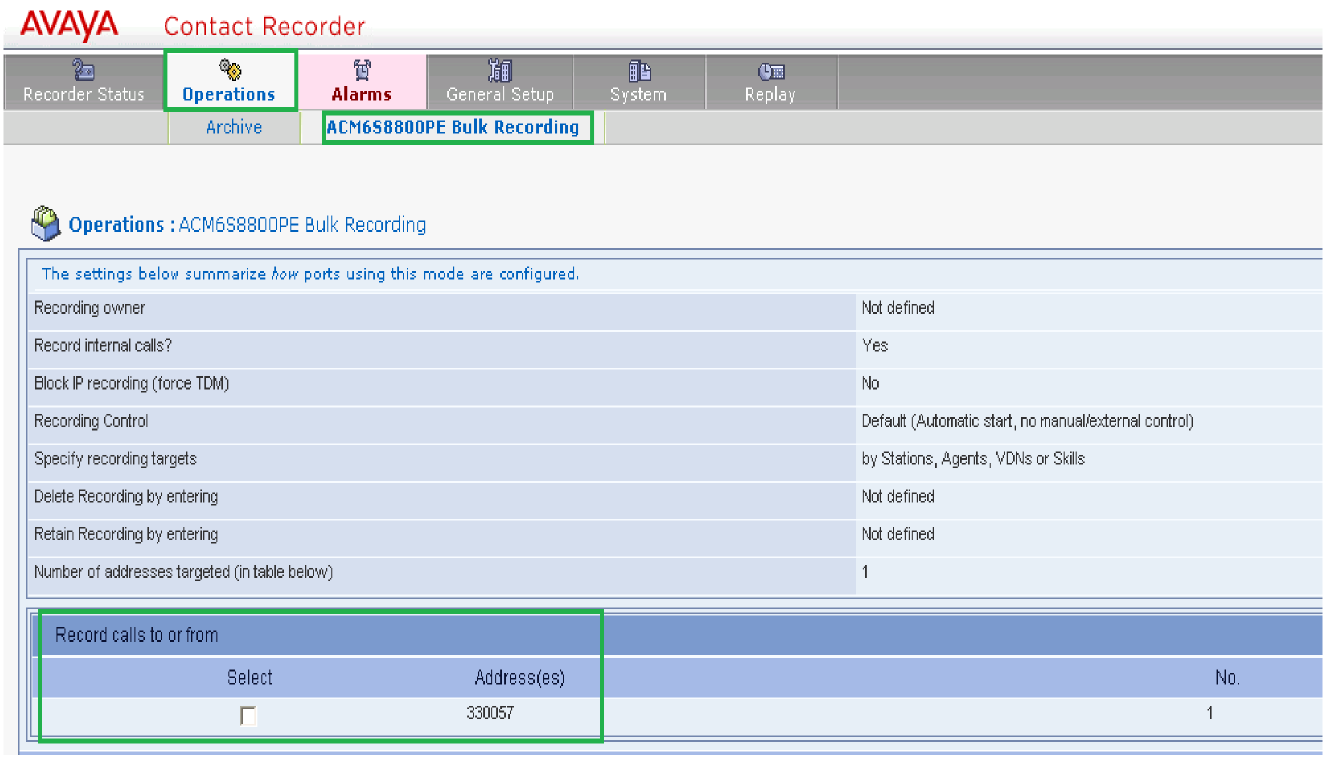
Step 2: General Setup for Avaya 33xxxxATL

Configure user credentials needed to connect to AES server for active CTI link and assign dedicated CMAPI ports



Step 3: Operations Level

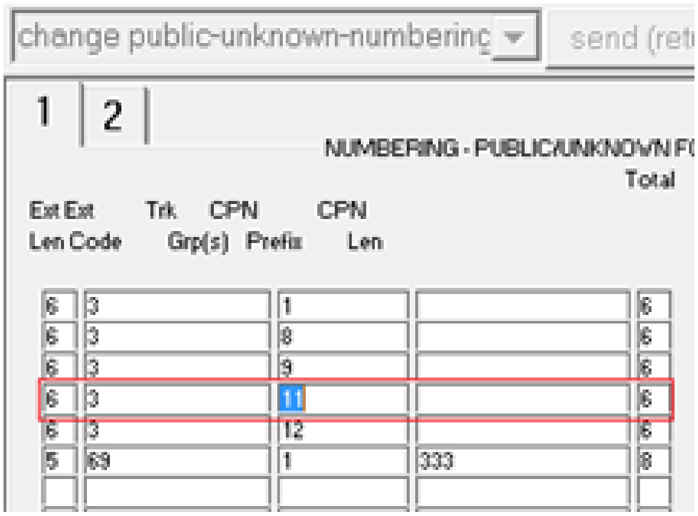
Configure bulk recording by assigning dedicated Avaya lines



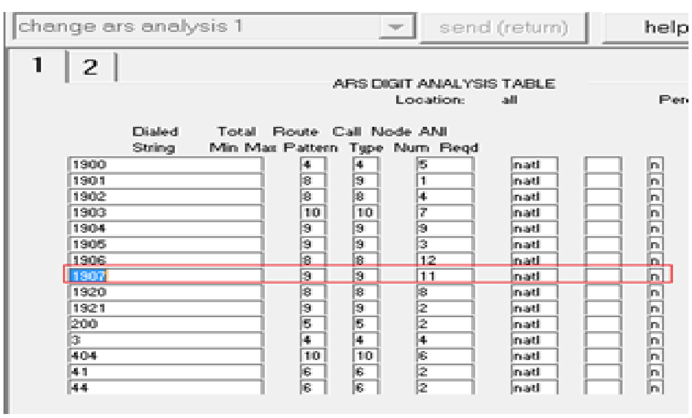
Avaya CM PBX Configuration Aspects

Step 1: Commands display setup on Avaya PBX, no Session-Manager used for this lab setup

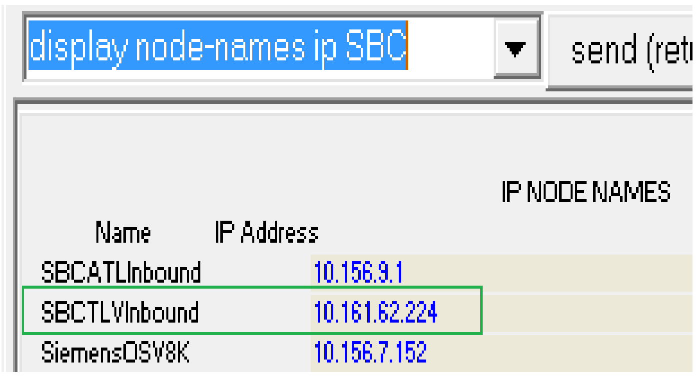
- change public-unknown-numbering 1



- change ars analysis 1

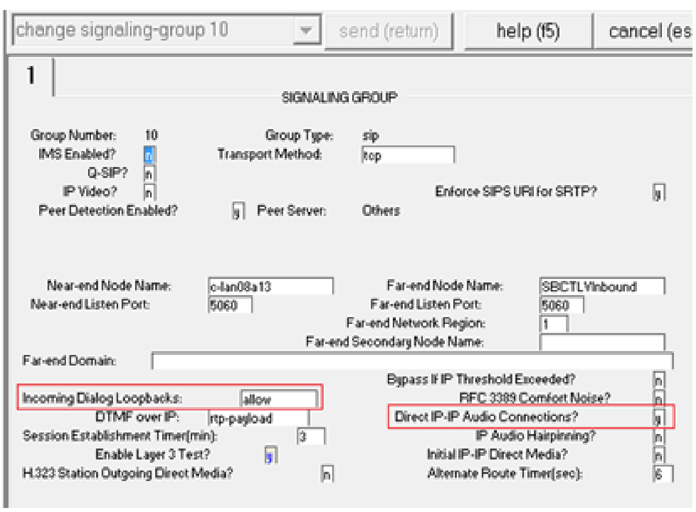


- display node-names ip SBC

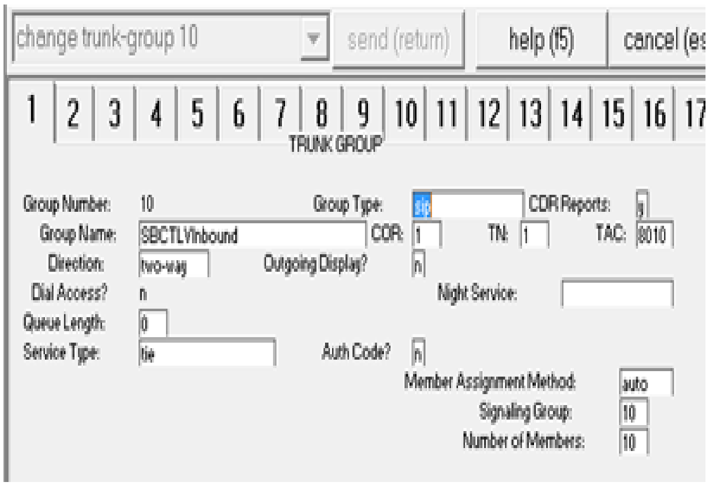


Step 2: Set up same signaling-group 10 to support both SIP trunks 10 (Inbound calls) and 11 (Outbound calls)

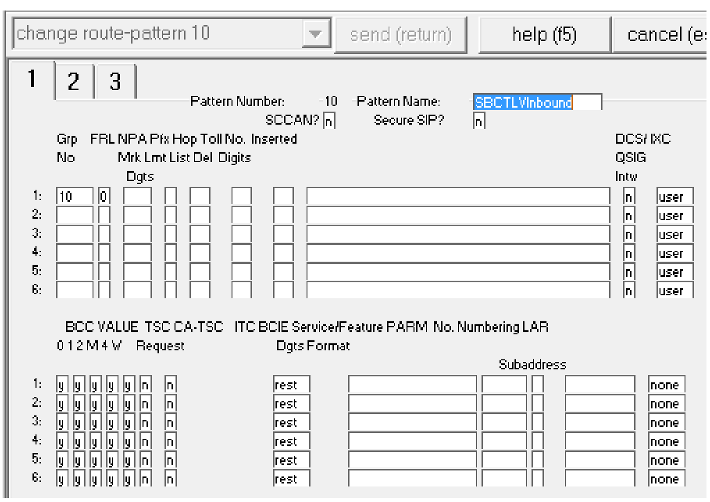
- change signaling-group 10

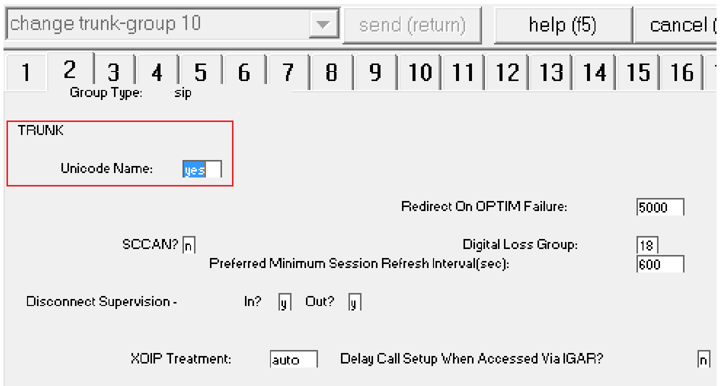


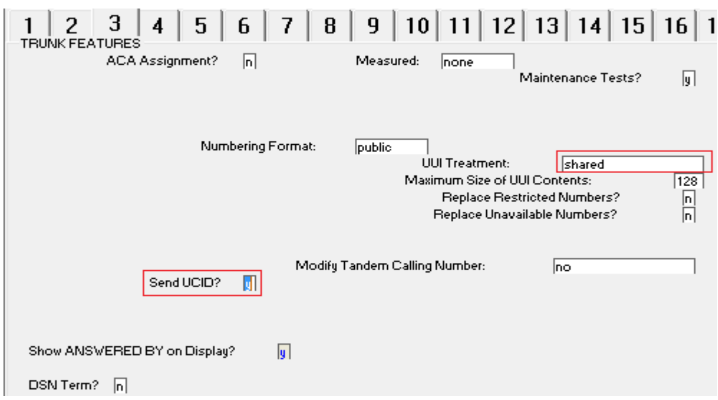
- change trunk-group 10



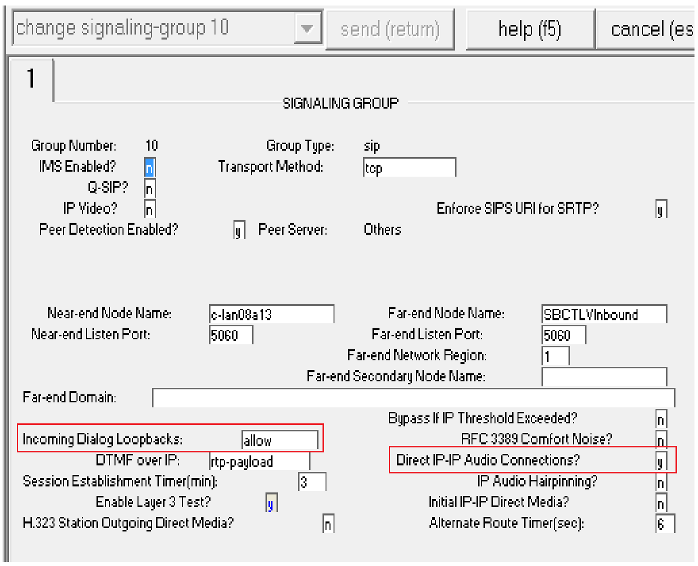
- change route-pattern 10



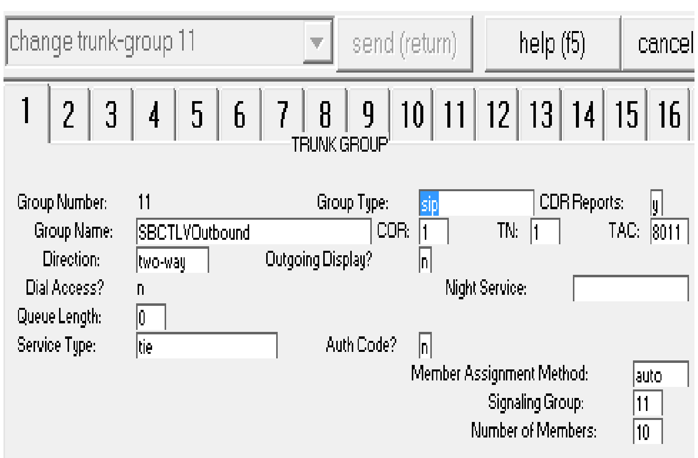




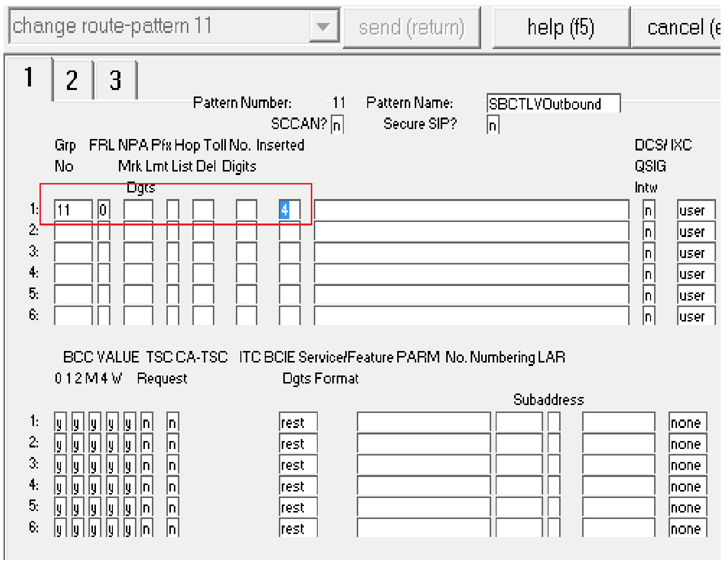
- change signaling-group 10

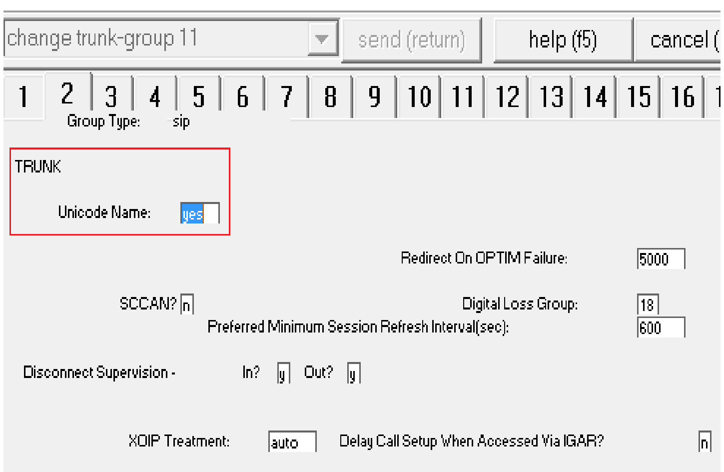


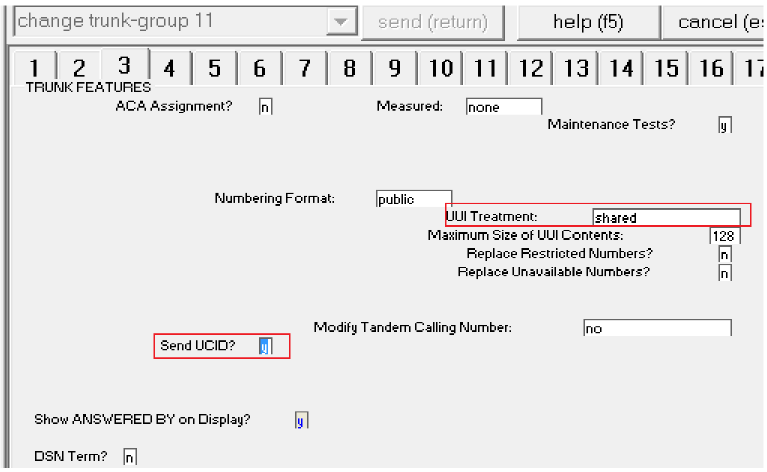
- change trunk-group 11



- change route-pattern 11


change route-pattern 11
send (return)
help (f5)
cancel (e
1 2 3
Pattern Number: 11 Pattern Name: SBCTLVOutbound
SCCAN? n Secure SIP? n
Grp FRL NPA Pfx Hop Toll No. Inserted
No Mrk Lmt List Del Digits
Dgts
DCS/ IXC
QSIG
Intw
1: 11 0 4 n user
2: n user
3: n user
4: n user
5: n user
6: n user
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR
0 1 2 M 4 W Request
Dgts Format
Subaddress
1: y y y y y n n rest none
2: y y y y y n n rest none
3: y y y y y n n rest none
4: y y y y y n n rest none
5: y y y y y n n rest none
6: y y y y y n n rest none


change trunk-group 11
send (return)
help (f5)
cancel (
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1
Group Type: sip
TRUNK
Unicode Name: yes
Redirect On OPTIM Failure: 5000
SCCAN? n
Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
XOIP Treatment: auto
Delay Call Setup When Accessed Via IGAR? n



Cisco UCM PBX Configuration Aspects

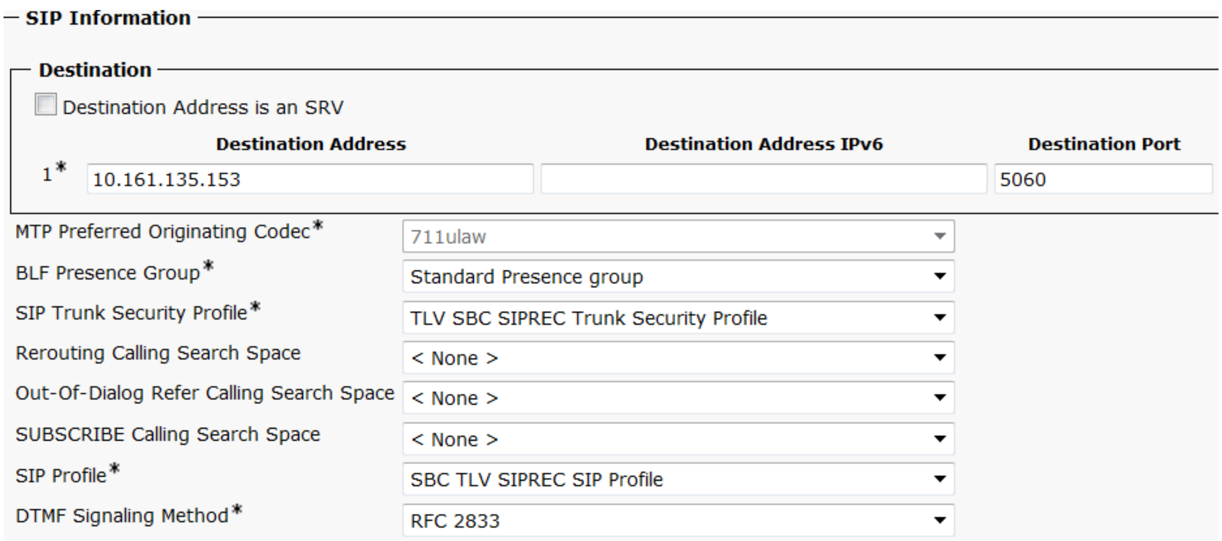
Step 1: Set up 2 dedicated SIP Trunks one for each dedicated network-interface on E-SBC configuration side

SBC_TLV_SIPREC_Inbound_from_ACM33xxxx	to SBC SOP0 10.161.62.224	Default		SIP Trunk	TLV SBC SIPREC Trunk Security Profile
SBC_TLV_SIPREC_Trunk_Outbound_to_ACM33xxxx	to SBC S0P1 10.161.135.153	Default	6.33XXXX	SIP Trunk	TLV SBC SIPREC Trunk Security Profile

Step 2: Inbound Calls through S0P0

Step 3: Outbound Calls through S0P1

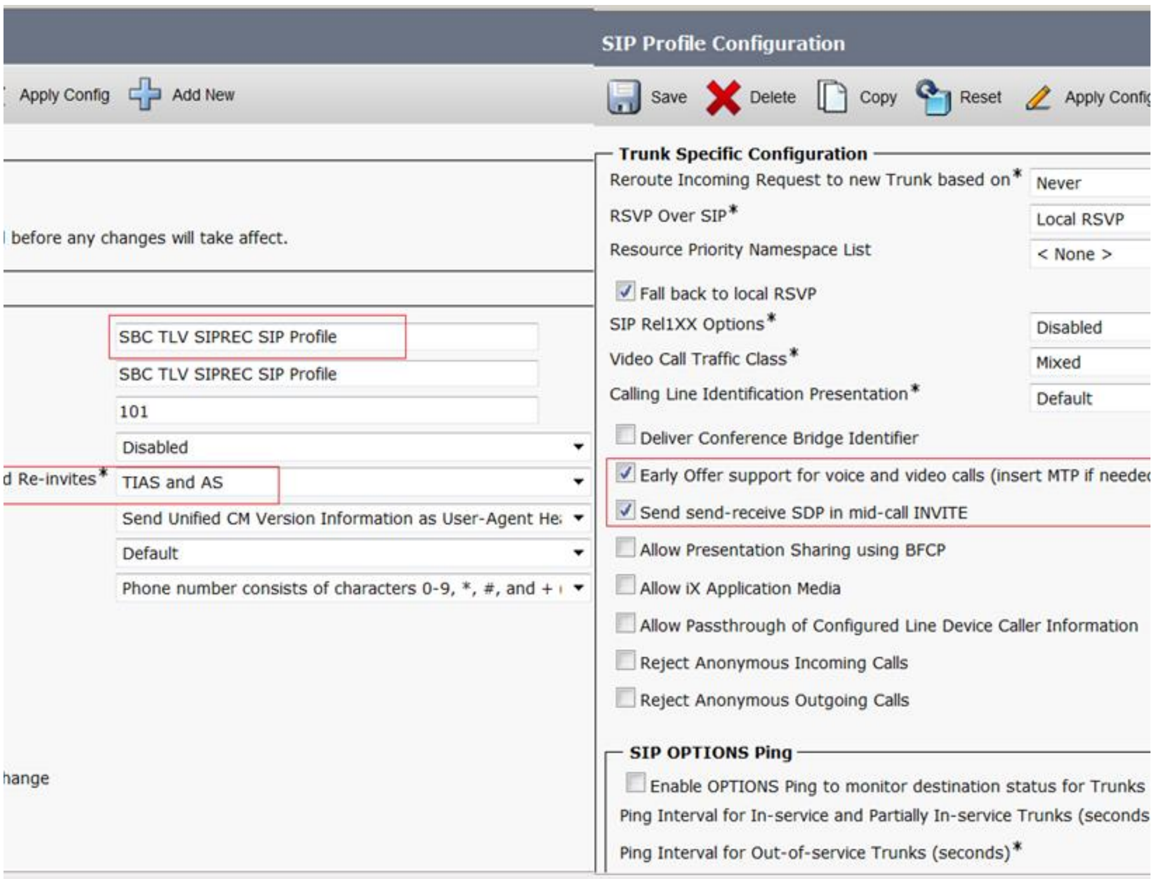
SBC_TLV_SIPREC_Trunk_Outbound_to_ACM33xxxx	to SBC S0P1 10.161.135.153	Default	6.33XXXX	SIP Trunk	TLV SBC SIPREC Trunk Security Profile



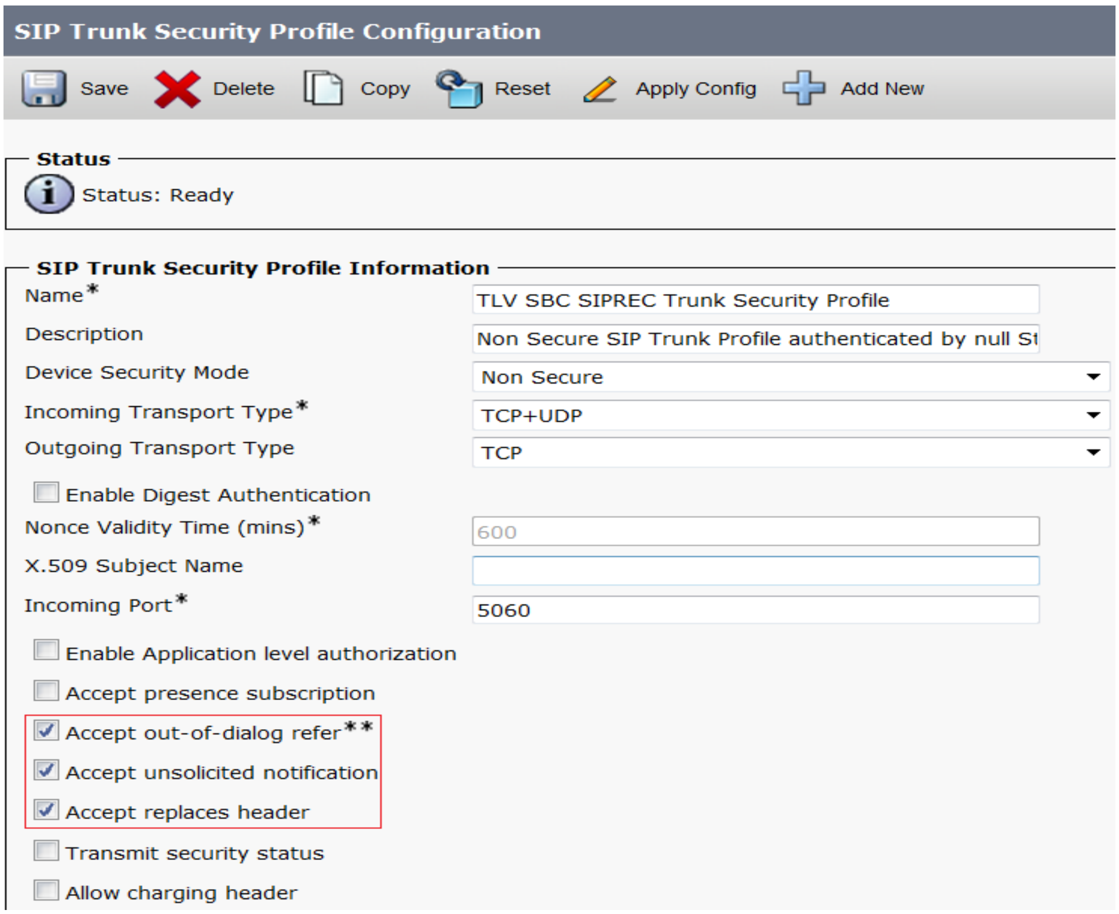
Step 4: Route pattern

6.33XXXX	Route through SBC TLV SIPREC to ACM33xxxx	SBC_TLV_SIPREC_Trunk

Step 5: SIP Profile



Step 6: SIP Trunk Security Profile


SIP Trunk Security Profile Configuration
Save
Delete
Copy
Reset
Apply Config
Add New
Status
Status: Ready
SIP Trunk Security Profile Information
Name*
TLV SBC SIPREC Trunk Security Profile
Description
Non Secure SIP Trunk Profile authenticated by null St
Device Security Mode
Non Secure
Incoming Transport Type*
TCP+UDP
Outgoing Transport Type
TCP
Enable Digest Authentication
Nonce Validity Time (mins)*
600
X.509 Subject Name
Incoming Port*
5060
Enable Application level authorization
Accept presence subscription
Accept out-of-dialog refer**
Accept unsolicited notification
Accept replaces header
Transmit security status
Allow charging header

Test Plan Executed

Following is the test plan executed against this setup and the results have been documented below.

Test ID	Task	Description	Steps		Status
441238	Validate SIP Tester Tool	Tag recording custom data from SIPREC metadata for SIPREC adapter	Step 1	Create an xml file with duplicate attributes in different paths	QA Preparation
			Step 2	map each of the duplicate attributes to a different field in the siprec adapter attributes page	
			Step 3	using the tester run the duplicate attributes xml file	
			Step 4	look at the log and make sure each of the two attributes got value from the xml file	
			Step 5	repeat the same scenario for nested attribute - the attribute is inside several layers of attributes	
			Step 6	Repeat the same scenario with different attributes	
			Step 7	delete an adapter attribute configuration and run the same xml file as previous step. make sure the attribute was NOT tagged and the changes took into effect immediately.	
441239	Configuration	Tag recording custom data from SIPREC metadata for SIPREC	Step 1	Install the latest KB	QA Preparation
			Step 2	Create Generic DS	
			Step 3	Create SIPREC adapter	

		adapter	Step 4	From command line run the "srat" batch file	
			Step 5	Copy the sip rec tester to the contact store	
			Step 6	in the sip rec adapter map extensiondata.rs_source.type to agent name	
			Step 7	from the testing tool send invite and this file name: invite,C:\Users\rs\Desktop\SRAT.v2\CustomAttrXMLTestNestedAttributes.xml	
			Step 8	make sure this log line is seen: [ProxyRecor|15F4|H] 2013-11-14 10:51:44.489-05:00 Recording<SIP/325/MixedHandset> tagged<AgentName, wowwow>	
441441	Basic Call (Agent)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent will click the release button on the phone device	
441442	Basic Call with Hold and Return (Agent)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold	
			Step 3	Agent returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441443	Agent Consults Another Available	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved

	Agent (Agent 1_Agent 1)		Step 2	Agent places caller on hold and makes a consultation call	
			Step 3	Agent disconnects from the Consultation call and returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441444	Agent Transfers Call To Another Agent-[non blind_transfer key] (Agent)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Transfer button which will transfer the caller to 2nd agent	
			Step 3	Agent will click the release button on the phone device	
441445	Agent Transfers Call To Another Agent-[blind_transfer key] (Agent)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent Agent presses the Transfer button again before the 2nd agent answers (blind transfer) which will transfer the caller to 2nd agent	
			Step 3	Agent2 picks up transferred call.	

			Step 4	Agent2 will click the release button on the phone device	
441446	Agent Conferences In Another Agent-[non blind_conference key] (Agent 1_Agent 2)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Conference button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Conference button which will conference all parties	
			Step 3	Agent1 talks and then presses 'release' button on phone device	
			Step 4	Agent2 remains talking and will click the release button on the phone device	
441447	Agent Conferences In Another Agent-[blind_conference key] (Agent 1_Agent 2)	Test Call scenarios while TSAPI is up	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Conference button Agent dials extension of another agent Agent presses the Conference button again before the 2nd agent answers (blind conference) which will conference all parties Agent2 answers the call	

			Step 3	Agent1 talks and presses 'release' button on phone device	
			Step 4	Agent2 remains talking and will click the release button on the phone device	
441448	Basic Outbound call	Test Call scenarios while TSAPI is up	Step 1	Agent makes an outbound call. (not Agent-to-Agent call) For example, if Avaya phone is the phone we are monitoring, then, make outbound call from Avaya to Nortel phone.	Approved
			Step 2	Agent releases the call.	
441449	Basic Call (Agent)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent will click the release button on the phone device	
441450	Basic Call with Hold and Return (Agent)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold	
			Step 3	Agent returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441451	Agent Consults Another Available Agent (Agent 1_Agent	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold and makes a consultation call	

	1)		Step 3	Agent disconnects from the Consultation call and returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441452	Agent Transfers Call To Another Agent-[non blind_transfer key] (Agent)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Transfer button which will transfer the caller to 2nd agent	
			Step 3	Agent will click the release button on the phone device	
441453	Agent Transfers Call To Another Agent-[blind_transfer key] (Agent)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent Agent presses the Transfer button again before the 2nd agent answers (blind transfer) which will transfer the caller to 2nd agent	
			Step 3	Agent2 picks up transferred call.	
			Step 4	Agent2 will click the release button on the phone device	

441454	Agent Conferences In Another Agent-[non blind_conference key] (Agent 1_Agent 2)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Conference button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Conference button which will conference all parties	
			Step 3	Agent1 talks and then presses 'release' button on phone device	
			Step 4	Agent2 remains talking and will click the release button on the phone device	
441455	Agent Conferences In Another Agent-[blind_conference key] (Agent 1_Agent 2)	Test Call scenarios while TSAPI adapter is down	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Conference button Agent dials extension of another agent Agent presses the Conference button again before the 2nd agent answers (blind conference) which will conference all parties Agent2 answers the call	
			Step 3	Agent1 talks and presses 'release' button on phone device	

			Step 4	Agent2 remains talking and will click the release button on the phone device	
441456	Basic Outbound call	Test Call scenarios while TSAPI adapter is down	Step 1	Agent makes an outbound call. (not Agent-to-Agent call) For example, if Avaya phone is the phone we are monitoring, then, make outbound call from Avaya to Nortel phone.	Approved
			Step 2	Agent releases the call.	
441457	Fallback is set to Application	Fallback Testing	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA Preparation
			Step 2	Set the MG fallback to Application	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is not being kept	
441458	Fallback is set to Performance	Fallback Testing	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA Preparation
			Step 2	Set the MG fallback to Performance	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is not being kept	

			Step 6	Turn off the TSAPI adapter	
			Step 7	Make the same call again	
			Step 8	Make sure the call is kept	
441459	Fallback is set to Liability	Fallback Testing	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA Preparation
			Step 2	Set the MG fallback to Liability	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is being kept	
441460	Configuration	Configuration	Step 1	Create one RIS and two recorders	QA Preparation
			Step 2	Associate RIS to the two recorders	
			Step 3	Create Avaya DS and assign it to the RIS	
			Step 4	Create a Gateway Side Correlation Pool MG and assign it to two MG	
			Step 5	Create 2 extensions 330025-330026	
			Step 6	Create LAN DS and connect it to the RIS	
			Step 7	Create Workstation Group and connect it to one of the servers	
			Step 8	Create two workstations - ie-scclient1/2	
			Step 9	Create two agents, connect the agents to both phones and workstations	
			Step 10	Create a BR that will trigger the screen	

			Step 11	Create SIPREC adapter and a TSAPI adapter	
441461	Basic Call (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent will click the release button on the phone device	
441462	Basic Call with Hold and Return (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold	
			Step 3	Agent returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441463	Agent Consults Another Available Agent (Agent 1_Agent 1)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold and makes a consultation call	
			Step 3	Agent disconnects from the Consultation call and returns to the caller	
			Step 4	Agent will click the release button on the phone device	
441464	Agent Transfers Call To Another Agent-	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent makes a consultation call	

	[non blind_2nd Line-Agent 2] (Agent)		Step 3	Agent presses the Transfer button Agent selects the extension on which the caller is on hold Agent presses the Transfer button again which will transfer the caller to 2nd agent	
			Step 4	Agent 2 talks and will click the release button on the phone device	
441465	Agent Conferences In Another Agent-[non blind_2nd Line-Agent2] (Agent 1_Agent 2)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold and makes a consultation call. Agent2 answers the call.	
			Step 3	Agent presses the conference button Agent selects the extension on which the caller is on hold Agent presses the conference button again which will conference all parties	
			Step 4	Agent1 releases	
			Step 5	Agent2 releases	
441466	Agent Conferences In Another Agent-[blind_2nd Line] (Agent	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold and makes a consultation call. Agent2 will not answer at this step.	

	1_Agent 2)		Step 3	Agent presses the conference button Agent selects the extension on which the caller is on hold Agent presses the conference button again which will conference all parties	
			Step 4	Agent2 answers the call.	
			Step 5	Agent1 releases	
			Step 6	Agent2 releases	
441467	Basic Outbound call	Call Scenarios	Step 1	Agent makes an outbound call. (not Agent-to-Agent call) For example, if Avaya phone is the phone we are monitoring, then, make outbound call from Avaya to Nortel phone.	Approved
			Step 2	Agent releases the call.	
441468	N Recorder Stopped	Failovers	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the N recorder	
			Step 3	Stop the ipcapture service	
			Step 4	Make a second call	
			Step 5	Make sure it is recorded on the M-shared recorder	
441469	N Recorder Re-Started	Failovers	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the N recorder	
			Step 3	Restart the ipcapture service	

			Step 4	Make a second call while the ip capture is restarting	
			Step 5	Make sure it is recorded on the M-shared recorder, stop the call	
			Step 6	Stop the M-Shard recorder	
			Step 7	Make a third call after the ipcapture is fully up	
			Step 8	Make sure the call gets recorded on the N-dedicated recorder	
441470	M Recorder Stopped	Failovers	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the M recorder	
			Step 3	Stop the M-Shard recorder	
			Step 4	Make another call	
			Step 5	Make sure the call gets recorded on the N-dedicated recorder	
441471	M Recorder Restart	Failovers	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the M recorder	
			Step 3	Stop the M-Shard recorder	
			Step 4	Make another call	
			Step 5	Make sure the call gets recorded on the N-dedicated recorder	
			Step 6	Bring back the M recorder and stop the N recorder	
			Step 7	Make sure the call gets recorded on the N recorder	

448453	Configuration	SIPREC Configuration	Step 1	Create an Avaya DS	QA Preparation
			Step 2	Create GSCP MG	
			Step 3	Create two extensions - 330025 & 330026	
			Step 4	Configure the NIC card to delivery and give a range of ports	
			Step 5	Create a SIPREC adapter (make sure the SBC is sending packets to this ip)	
			Step 6	Create TSAPI adapter AVAYA#ACM6S8800PE#CSTA#QAAESERVICES6X	
448480	Basic Call (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent will click the release button on the phone device	
448481	Basic Call with Hold and Return (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold	
			Step 3	Agent returns to the caller	
			Step 4	Agent will click the release button on the phone device	
448482	Agent Consults Another Available Agent (Agent 1_Agent 1)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent places caller on hold and makes a consultation call	
			Step 3	Agent disconnects from the Consultation call and returns to the caller	

			Step 4	Agent will click the release button on the phone device	
448483	Agent Transfers Call To Another Agent-[non blind_transfer key] (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Transfer button which will transfer the caller to 2nd agent	
			Step 3	Agent will click the release button on the phone device	
448484	Agent Transfers Call To Another Agent-[blind_transfer key] (Agent)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Transfer button Agent dials extension of another agent Agent presses the Transfer button again before the 2nd agent answers (blind transfer) which will transfer the caller to 2nd agent	
			Step 3	Agent2 picks up transferred call.	
			Step 4	Agent2 will click the release button on the phone device	
448485	Agent Conferences In Another	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved

	Agent-[non blind_conference key] (Agent 1_Agent 2)		Step 2	Agent presses the Conference button Agent dials extension of another agent 2nd agent Answers call 1st agent presses the Conference button which will conference all parties	
			Step 3	Agent1 talks and then presses 'release' button on phone device	
			Step 4	Agent2 remains talking and will click the release button on the phone device	
448486	Agent Conferences In Another Agent-[blind_conference key] (Agent 1_Agent 2)	Call Scenarios	Step 1	Place a call which will route to the agent's phone device	Approved
			Step 2	Agent presses the Conference button Agent dials extension of another agent Agent presses the Conference button again before the 2nd agent answers (blind conference) which will conference all parties Agent2 answers the call	
			Step 3	Agent1 talks and presses 'release' button on phone device	
			Step 4	Agent2 remains talking and will click the release button on the phone device	

448487	Basic Outbound call	Call Scenarios	Step 1	Agent makes an outbound call. (not Agent-to-Agent call) For example, if Avaya phone is the phone we are monitoring, then, make outbound call from Avaya to Nortel phone.	Approved
			Step 2	Agent releases the call.	
448488	Fallback is set to Application	APL Modes	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA Preparation
			Step 2	Set the MG fallback to Application	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is not being kept	
448489	Fallback is set to Performance	APL Modes	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA preparation
			Step 2	Set the MG fallback to Performance	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is not being kept	
			Step 6	Turn off the TSAPI adapter	
			Step 7	Make the same call again	
			Step 8	Make sure the call is kept	

448490	Fallback is set to Liability	APL Modes	Step 1	Setup Avaya SIPREC system with DS, MG and extensions 330026/7	QA Preparation
			Step 2	Set the MG fallback to Liability	
			Step 3	Set Avaya TSAPI adapter and sip proxy adapter	
			Step 4	Make a call to an unmonitored 33xxxx extension so it will route through the ACME SBC	
			Step 5	Hangup the call and make sure it is being kept	
448493	N Recorder Stopped	N+M Testing	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the N recorder	
			Step 3	Stop the ipcapture service	
			Step 4	Make a second call	
			Step 5	Make sure it is recorded on the M-shared recorder	
448494	N Recorder Re-Started	N+M Testing	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the N recorder	
			Step 3	Restart the ipcapture service	
			Step 4	Make a second call while the ip capture is restarting	
			Step 5	Make sure it is recorded on the M-shared recorder, stop the call	
			Step 6	Stop the M-Shard recorder	
			Step 7	Make a third call after the ipcapture is fully up	

			Step 8	Make sure the call gets recorded on the N-dedicated recorder	
448495	M Recorder Stopped	N+M Testing	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the M recorder	
			Step 3	Stop the M-Shard recorder	
			Step 4	Make another call	
			Step 5	Make sure the call gets recorded on the N-dedicated recorder	
448496	M Recorder Restart	N+M Testing	Step 1	Configure the system to record in N+M configuration	QA Preparation
			Step 2	Make a call, make sure it is recorded on the M recorder	
			Step 3	Stop the M-Shard recorder	
			Step 4	Make another call	
			Step 5	Make sure the call gets recorded on the N-dedicated recorder	
			Step 6	Bring back the M recorder and stop the N recorder	
			Step 7	Make sure the call gets recorded on the N recorder	
448497	Configura tion - Dialer Regressi on	Dialer Testing	Step 1	Configure Avaya SBC to send SIPRec packets to the recorder	QA Preparation
			Step 2	Configure Aspect UIP Dialer DS and link it to the Avaya DS	
			Step 3	Configure GSCP MG. Configure extension - 330025	

			Step 4	Configure Screen DS with WSG and workstation and link it to the phone extension	
			Step 5	Configure a SIPRec and TSAPI adapters for the Avaya DS	
			Step 6	Configure Concerto Adapter for the Aspect UIP DS	
448498	Regression - Dialer Calls	Dialer Testing	Step 1	Make a call using the SBC from cisco 90xxx to Avaya 330025	QA Preparation
			Step 2	Make sure both screen and audio are recorded	
			Step 3	Using netcat send agent logon, Open the RM and query RIS to see that a workspace with the agent is present	
			Step 4	Send startcall using netcat, make sure that both audio and screen recording break, a new recordings starts and that RIS log indicates that a nail-up call was detected	
			Step 5	Send stop call and hang up the call	
			Step 6	Open the Portal and make sure the call is tagged and the call direction is outbound	
448499	Review documentation	Documentation	Step 1	Review documentation for SIPREC	QA Preparation

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 Oracle E-SBC 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.

Since we are concerned with communication between the Verint Recorder and the E-SBC we will focus on the troubleshooting tools to use between those devices if calls are not working or tests are not passing.

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org.

On the Oracle E-SBC

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

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

At the E-SBC Console:

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

Examining the log files.

Note: You will FTP to the management interface of the E-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 ACMESYSTEM FTP 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.

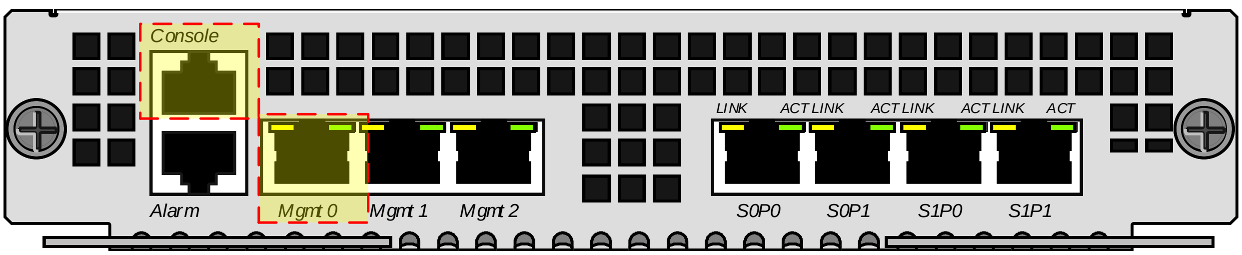
Appendix A

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, this must be explicitly configured.

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

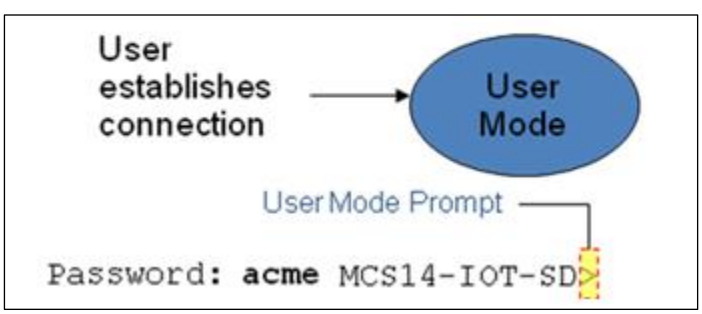


ACLI Basics

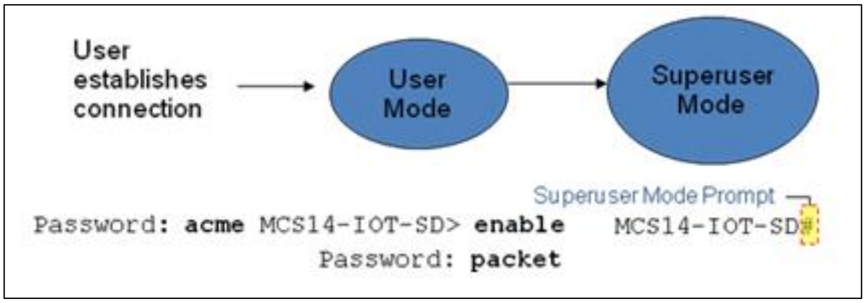
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the E-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.



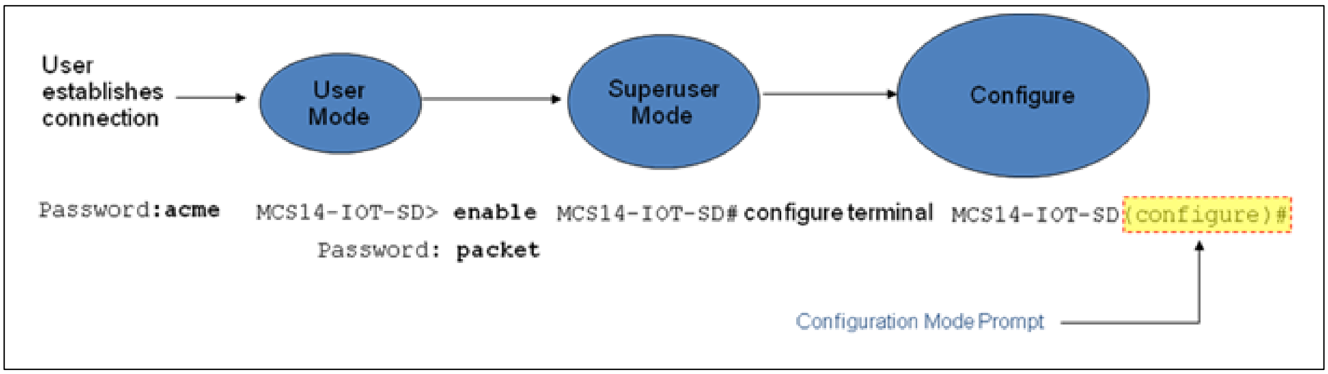
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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.

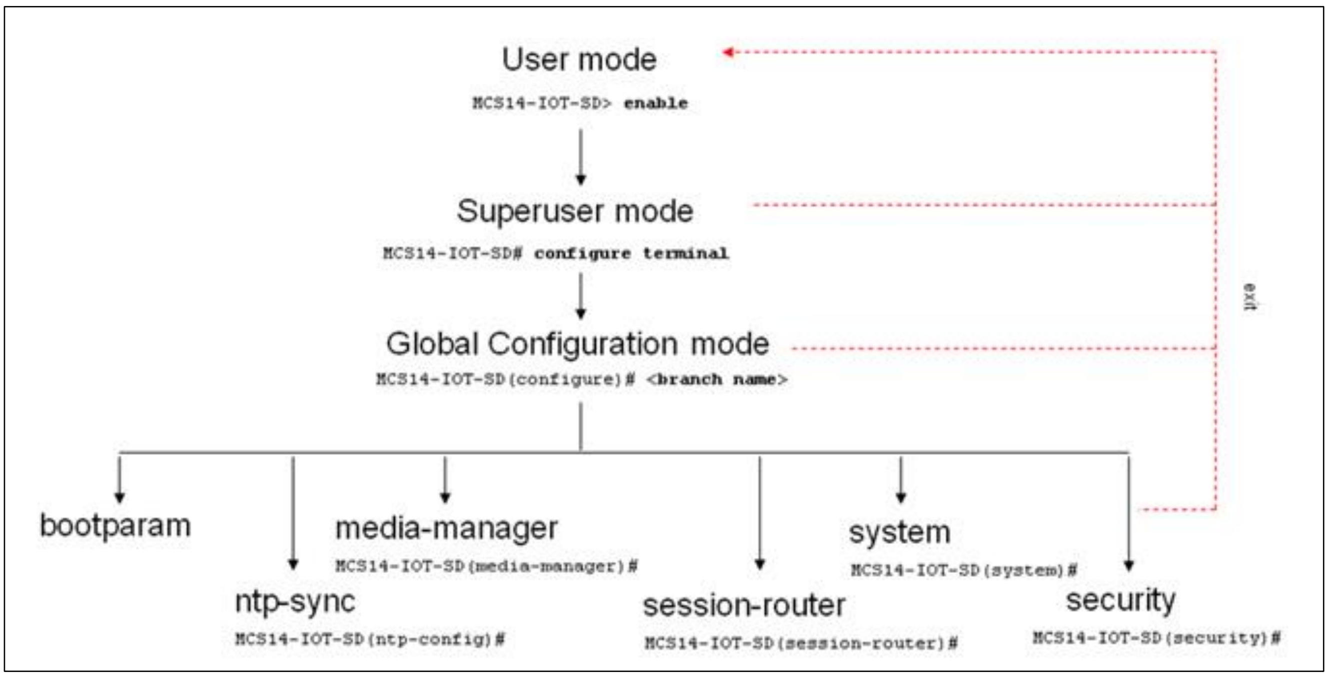
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **ACMESYSTEM(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 E-SBC boot parameters. Key boot parameters include:

- boot device – The global management port, usually eth0
- file name – The boot path and the image file.

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

```
'.' = clear field;  '-' = go to previous field;  q = quit
boot device              : eth0
processor number         : 0
host name                :
file name                : /tffs0/nnSCX620.gz
inet on ethernet (e)     : 10.0.3.11:ffff0000
inet on backplane (b)    :
host inet (h)            : 10.0.3.100
gateway inet (g)         : 10.0.0.1
user (u)                 : anonymous
ftp password (pw) (blank = rsh)      : anonymous
flags (f)                : 0x8
target name (tn)         : MCS14-IOT-SD
startup script (s)       :
other (o)
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the E-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 E-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 E-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 E-SBC reboots, your configurations will be lost.

Configuration Versions

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

```
MCS14-IOT-SD# 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'.
MCS14-IOT-SD#
```

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 E-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.

```
MCS14-IOT-SD# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
MCS14-IOT-SD#
```

ORACLE

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com