ORACLE
COMMUNICATIONS

ORACLE

Oracle Enterprise Session Border Controller and Semafone PCI Compliance Solution Interoperability Testing in a Contact Center Environment

Technical Application Note

ORACLE

Disclaimer

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

Table of Contents

Intended Audience

This document is intended for use by Oracle personnel, 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. There will be steps that require navigating the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Document Overview

This document provides an overview of the interoperability testing environment and tests that will be conducted to determine the recommended configuration for the Oracle Communications E-SBC and the Semafone PCI Compliance Solution when deployed into a contact center environment.

Introduction

Oracle Communication Enterprise Session Border Controllers (E-SBCs) enable contact centers to accelerate the adoption of real-time IP communications by removing common security, interoperability, and reliability barriers. E-SBCs are fundamental network infrastructure components that enable real-time voice, video, instant messaging, and Unified Communications (UC) to be extended across network boundaries. E-SBCs make it possible for enterprises to replace legacy time division multiplexing (TDM) contact center networks with more-efficient Session Initiation Protocol (SIP)–based networks to reduce capital expenditures and operating expenses and to transform conventional brick-and-mortar call centers into virtual contact centers that incorporate remote agents and cloud-based services to increase productivity and improve business agility.

Semafone provides secure voice transactions for contact centers and retailers taking Cardholder Not Present (CNP) payments. The Semafone solution allows a call to continue as normal whilst the customer enters their credit card information using their telephone keypad. Semafone's patented technology masks the Dual Tone Multi-Frequency (DTMF) tones from the cardholder's telephone and replaces them with a flat tone so they can't be recognized by the call center agent. By ensuring all card data remains segregated and by removing Sensitive Authentication Data (SAD) before it hits the contact center infrastructure, the contact center is taken out of the scope of PCI DSS, protected against the risk of opportunistic agent fraud and the associated reputational risk.

Requirements

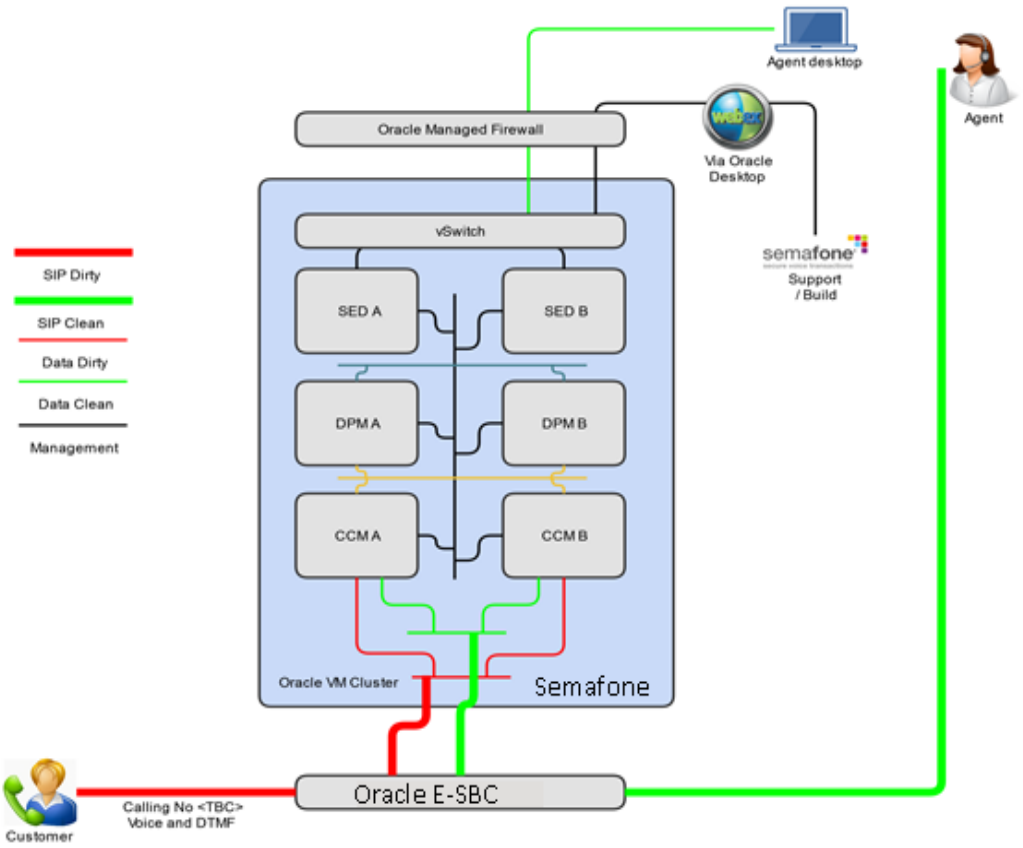
- Fully functioning Semafone application. The version tested as part of this interop is Semafone 3.2.0.0.
- Oracle Enterprise Session Border Controller running ECZ730m1p1. Note: the configuration running on the SBC is backward/forward compatible with any release in the 7.3.0 & 7.4.0 stream. If using platforms 4500/3820, a transcoding NIU will be required for this implementation. The interoperability tests were conducted using a 3820 platform however the same feature support is available on the following E-SBC models:
    - 1100
    - 3820 w/ Transcoding NIU
    - 4500 w/ Transcoding NIU
    - 3900
    - 4600 &
    - 6300

Note:

Customers using existing E-SBC to align with PCI compliance, please note that session count would need to be doubled on the E-SBC as each of the PCI calls will need to be routed in & out to Semafone application before a call is delivered to your contact center application. Also ensure that the DSP requirement for transcoding on your NIU aligns with the total number of sessions required.

Architecture

The following reference architecture shows a logical view of the connectivity between the E-SBC and Semafone.



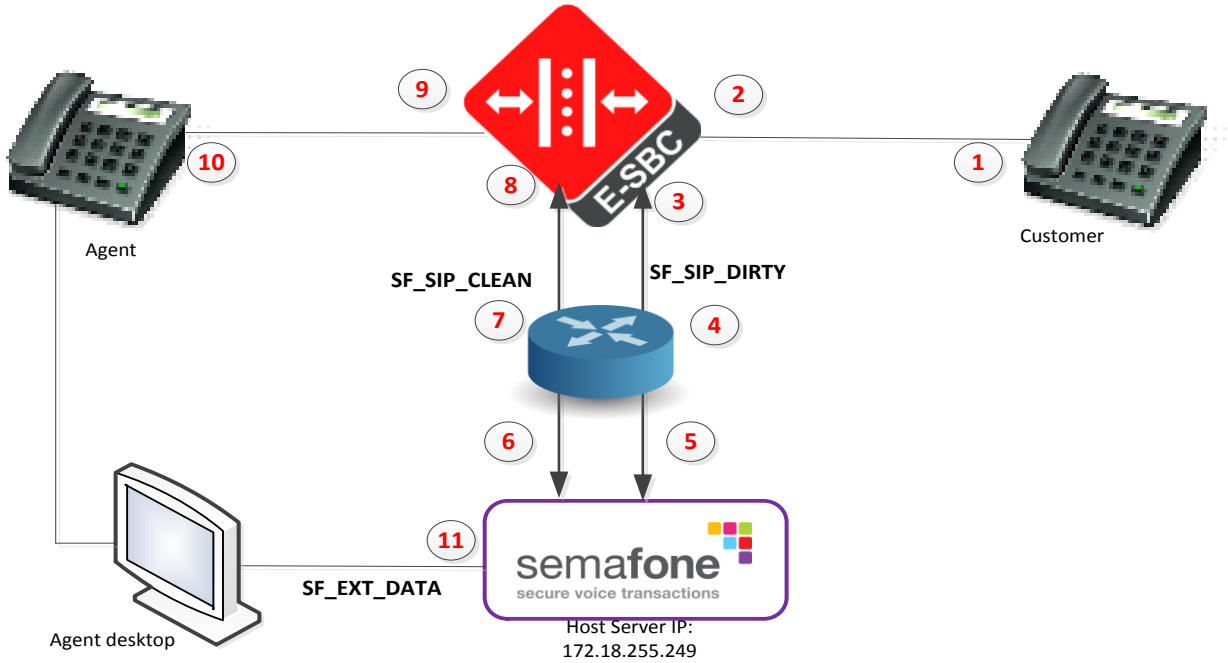
The Oracle E-SBC is deployed at the edge of an Enterprise which has a contact center. Semafone application is typically deployed inside the Enterprise core as well, and is connected to the E-SBC. For the purpose of this testing, we have used Bria soft clients instead of the contact center application.

When a customer calls a contact center agent and needs to make a payment, agent Initiated SecureMode will be used. A five digit call reference (CR) will be displayed to the agent on the Semafone standard payment page. When the agent wishes to enter SecureMode in order to take a payment, they must enter a prefix digit (#) followed by this number on their telephone keypad. This will pair the telephone line in use with the payment session that has been initiated and will place Semafone in SecureMode. The role of the E-SBC is to convert the DTMF tones it receives from the customer (Credit card number) into SIP INFO and send to Semafone. When in SecureMode, Semafone will mask the credit card number which it receives from the E-SBC with mono-tones that cannot be reverse engineered to reveal the secure card data. Semafone will then send the payment information to the Payment Gateway which is not in scope of this testing.

This document provides an overview of the interoperability testing environment and tests that have been conducted to determine the recommended configuration for the Oracle E-SBC and the Semafone system when deployed into a hosted (or large enterprise) environment.

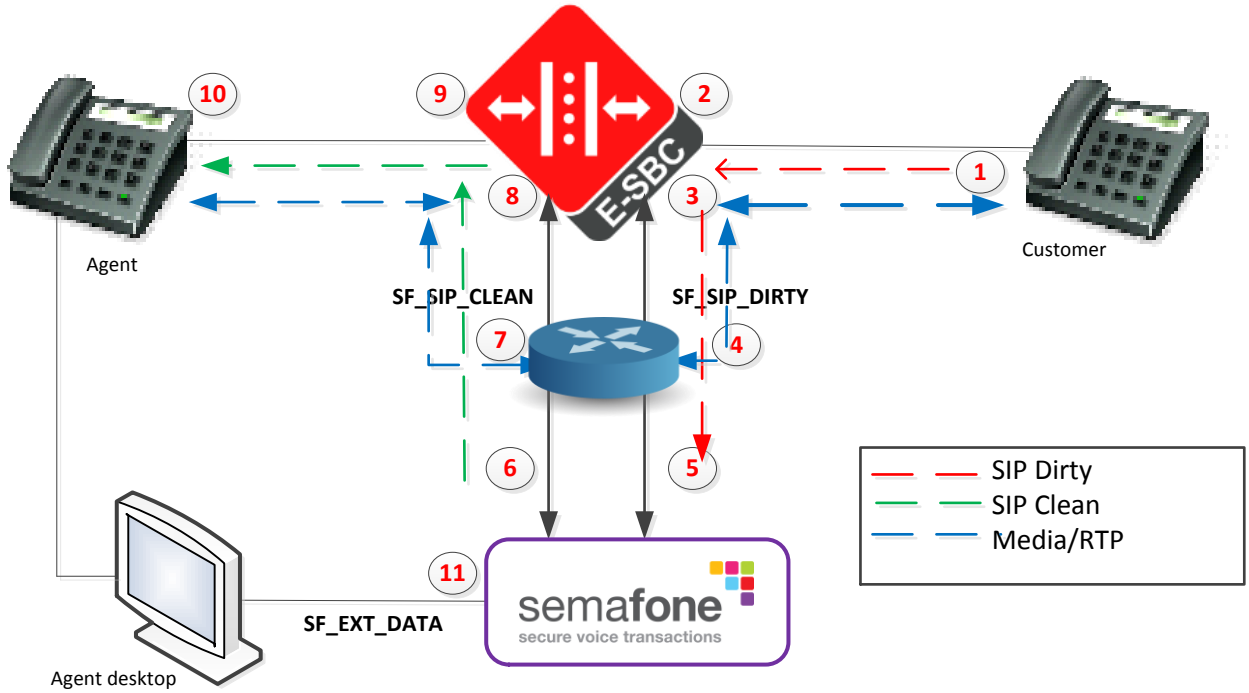
Lab Configuration

The following diagram, similar to the Reference Architecture described earlier in this document, illustrates the lab environment created to facilitate certification testing (IP addressing/Port below is only a reference, they can change per your network specification).



Number	Description	IP
1	Customer (softphone)	192.160.2.150/24
2	SBC Dirty interface facing Customer	192.160.2.200/24
3	SBC Dirty interface facing Semafone	172.16.5.193/28
4	Router interface on Dirty Network	172.16.5.195/28
5	Semafone Dirty VIP	172.16.5.200/28
6	Semafone Clean VIP	172.16.5.100/28
7	Router interface on Clean Network	172.16.5.105/28
8	SBC Clean interface facing Semafone	172.16.5.110/28
9	SBC Clean interface facing Agent	10.232.50.200/24
10	Agent (softphone)	10.232.50.211/24
11	Semafone External VIP	172.18.255.132/16

Call flow



When the customer calls the agent, the call flow is as shown above. The E-SBC is using four physical interfaces for the purpose of this testing, one for the Customer, one for agent, one each for Semafone Dirty and Semafone clean. SIP Dirty is the SIP signaling which contains the raw credit card and CVV digits, SIP Clean is after Semafone masks the credit card digits in the SIP messaging. The SP_EXT_DATA is the Semafone interface which exposes the Semafone APIs and routes traffic to a Payment Service Provider(PSP) or Payment Gateway. Please note Semafone does not handle the media/RTP; as shown above, media leaves the E-SBC from the SBC Dirty interface into the SBC clean interface through the router.

NOTE:

During SIP signaling negotiation between customer & agent – the Semafone application doesn't latch its IP as part of the SDP negotiation – this triggers the E-SBC to route all media using IPs negotiated (which are the two IPs associated with dirty/clean interfaces on E-SBC) within the SDP offer exchange. A key aspect for the solution to work requires the E-SBC to route the media (RTP) out of the E-SBC and back into the E-SBC on a different interface. The router (marked in blue) delivers this capability in the call flow - without the routing ability the calls wouldn't work as expected.

Configuring the Oracle Enterprise SBC

In this section we describe the steps for configuring an Oracle Enterprise SBC, formally known as an Acme Packet Net-Net Session Director ("SBC"), for use with Semafone.

In Scope

The following guide configuring the Oracle E-SBC assumes that this is a newly deployed device dedicated to a single customer. If a customer currently has the SBC deployed and is adding Semafone, then please see the ACLI Configuration Guide on http://docs.oracle.com/cd/E61547_01/index.html for a better understanding of the Command Line Interface (CLI).

Out of Scope

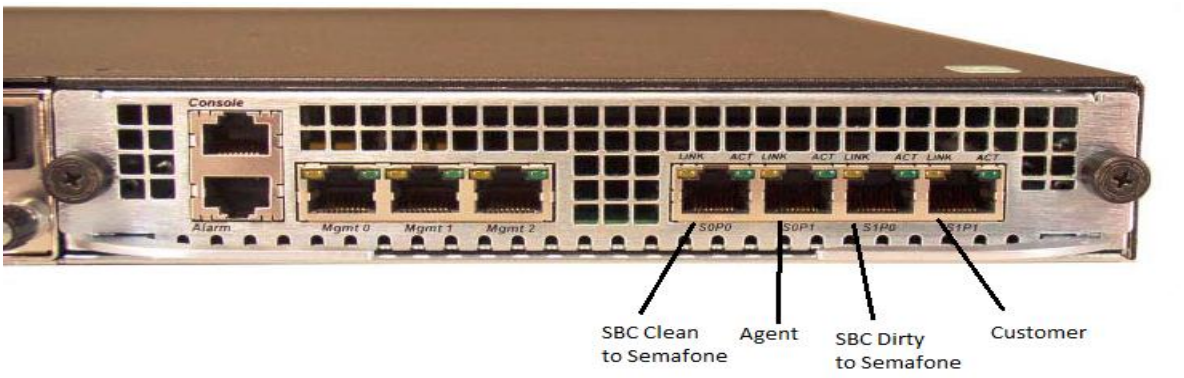
- Configuration of Network management including SNMP and RADIUS

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 SBC
- IP address to be assigned to management interface (Wancom0) of the SBC - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support SBC configurations with management and media/service interfaces on the same subnet.
- IP addresses of Semafone dirty and clean interfaces facing the E-SBC
- IP addresses to be used for the SBC internal (agent), external (customer) facing ports (Service Interfaces)

SBC Getting Started

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity. **Note: use the console port on the front of the SBC, not the one on the back.**



Plug the slot 0 port 0 (s0p0) interface into Semafone Clean interface, the slot 0 port 1(s0p1) into the Contact center agent facing network, slot 1 port 0(s1p0) into the Semafone Dirty interface and slot 1 port 1(s1p1) into the Customer facing network . Once connected, perform you are ready to power on and perform the following steps.

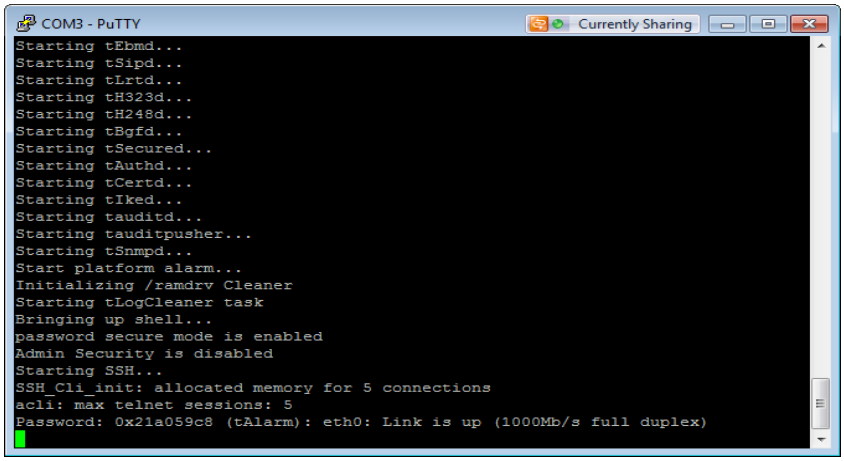
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as oraclesbc1 are parameters which are specific to an individual deployment. **Note:** The ACLI is case sensitive.

Establish the serial connection and logging in the SBC

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



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

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

You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

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

oraclesbc1#configure terminal --- >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 File             : /boot/nnECZ730m1p1.XX.bz
IP Address            : 192.65.79.44
VLAN                  :
Netmask               : 255.255.255.224
Gateway               : 192.65.79.33
IPv6 Address          :
IPv6 Gateway          :
Host IP               : 0.0.0.0
FTP username          : vxftp
FTP password          : vxftp123
Flags                 :
Target Name           : ACMESYSTEM
Console Device        : COM1
Console Baudrate      : 115200
Other                 :

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

Configuring the SBC

The following section walks you through configuring the Oracle Enterprise SBC required to work with Semafone. Semafone has two interfaces Clean and Dirty which are connected to the SBC on the same vlan (or routed to each other through Semafone network). When the customer punches in the credit card number, the E-SBC converts the DTMF received to SIP INFO and sends it to Semafone Dirty interface. The Semafone dirty interface receives the SIP INFO with the credit card digits and it masks the digits and sends them back to the SBC through the Clean interface.

The following testing has been conducted with G729b, G711 u-law and G711 a-law. The SBC uses codec-policies PCMUonly, G729only and PCMAonly to filter out the other codecs and force it to transcode the DTMF to SIP INFO. Depending on which codec is being tested, the corresponding codec-policy is applied in the realm-config.

Following config elements requires to altered from default value:

rfc2833-end-pkts-only-for-non-sig: Under media-manager-config . Change this parameter to disabled; this causes the SBC to send the start-interim-end RFC 2833 packets for non-signaled digit events

translate-non-rfc2833-event: Under media-manager-config. Change this parameter to enabled, this causes the E-SBC to always send the type of DTMF messages that were initially negotiated, regardless of the type of messages it may be receiving.

rfc2833-mode: This parameter in sip-interface is what causes the SBC to transcode the DTMF to SIP INFO and vice versa. It is set to preferred on the Agent and Customer realms, and set to dual on the Semafone clean and dirty realms for this testing.

Setting the sip-interface's rfc2833-mode to **preferred** indicates that the RFC 2833 telephone-event DTMF transfer method is the preferred method for sending a DTMF indication. In the capability negotiation phase a telephone-event media type will be inserted in the outgoing SDP offer, if it was not present in the original offer. If telephone-event was already present in the offer, then the E-SBC maintains the telephone-event support even if the next hop does not support RFC2833.

Consider the following scenario when a customer calls an agent; and when both of them support RFC2833. This is the scenario which has been tested as part of this interop.

- If the SIP trunk on the customer end supports RFC2833, the invite coming to the SBC will have telephone-event advertised in the SDP.
- The rfc2833-mode is set to **preferred** on the sip-interface facing the customer, so the E-SBC maintains the telephone-event support even though the next hop (in this case Semafone) does not.

- The rfc2833-mode is set to **dual** on the sip-interface facing the Semafone dirty interface. Dual means that the SBC will support both RFC2833 and SIPINFO. Since Semafone does not support RFC2833, the SBC will need to transcode the RFC2833 received from the customer to SIP INFO when sending to Semafone.
- The rfc2833-mode is set to **dual** on the sip-interface facing the Semafone clean side. When the SBC receives the SIP INFO back from Semafone clean interface, the next-hop is to the agent on which the rfc2833-mode is set to **preferred**.
- If the contact center also supports RFC2833, the rfc2833-mode set to **preferred** ensures that the E-SBC transcodes the SIP INFO received from Semafone clean to RFC2833.

Consider the following scenario when a customer calls agent; the SIP trunk on the customer side does not support RFC2833 while the contact center supports RFC2833.

- The INVITE coming from the customer will not have telephone-event in the SDP, in this case the rfc2833-mode in the sip-interface facing customer should be set to **transparent**.
- The rfc2833-mode set to **dual** on the sip-interface facing Semafone dirty will ensure that the SBC transcodes the DTMF received from the customer to SIP INFO.
- The rfc2833-mode is set to **dual** on the sip-interface facing Semafone clean; SBC will process the SIP INFO from Semafone clean.
- The rfc2833-mode set to **preferred** on the sip-interface facing the agent will add the telephone-event to the INVITE coming from the Semafone since the agent supports telephone-event.

respondINFO: This sip-manipulation is applied as an in-manipulationid to the Semafone dirty sip-interface. When the agent presses the CR code, Semafone masks those digits as well and sends the signal=E in the SIP INFO to the SBC. According to RFC2733, there is no definition for the event E, hence the SBC is not able to transcode this back to DTMF to send to the customer. Since this code is redundant for the customer anyways, the SBC responds with 200OK to the Semafone Dirty interface and drops the DTMF from going to the customer. This is a workaround.

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

SBC Configuration

Following is the configuration of the SBC:

```
codec-policy
        name                                    G729only
        allow-codecs                            G729 telephone-event
        add-codecs-on-egress
        dtmf-in-audio                           preferred
codec-policy
        name                                    PCMAonly
        allow-codecs                            PCMA telephone-event
        add-codecs-on-egress
        dtmf-in-audio                           preferred
codec-policy
        name                                    PCMUonly
        allow-codecs
        dtmf-in-audio                           preferred
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Agent
        policy-attribute
                next-hop                                172.16.5.100
                realm                                   Sema-clean
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Sema-clean
        policy-attribute
                next-hop                                10.232.50.211
                realm                                   Agent
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Sema-dirty
        policy-attribute
                next-hop                                192.160.2.150
                realm                                   Customer
local-policy
        from-address                            *
        to-address                              *
        source-realm                            Customer
        policy-attribute
                next-hop                                172.16.5.200
                realm                                   Sema-dirty
media-manager
        rfc2833-end-pkts-only-for-non-sig       disabled
        translate-non-rfc2833-event             enabled
network-interface
        name                                    s0p0
        ip-address                              172.16.5.110
        netmask                                 255.255.255.240
        gateway                                 172.16.5.105
        hip-ip-list                             172.16.5.110
        icmp-address                            172.16.5.110
network-interface
```

```
        name                                    s0p1
        ip-address                              10.232.50.200
        netmask                                 255.255.255.0
        gateway                                 10.232.50.89
        hip-ip-list                             10.232.50.200
        icmp-address                            10.232.50.200
        ssh-address                             10.232.50.210
network-interface
        name                                    s1p0
        ip-address                              172.16.5.193
        netmask                                 255.255.255.240
        gateway                                 172.16.5.195
        hip-ip-list                             172.16.5.193
        icmp-address                            172.16.5.193
network-interface
        name                                    s1p1
        ip-address                              192.160.2.200
        netmask                                 255.255.255.0
        gateway                                 192.160.2.50
        hip-ip-list                             192.160.2.200
        icmp-address                            192.160.2.200
        ssh-address                             192.160.2.200
network-interface
        name                                    wancom1
        description                             HA_HEARTBEAT1
        pri-utility-addr                        169.254.1.1
        sec-utility-addr                        169.254.1.2
        netmask                                 255.255.255.252
network-interface
        name                                    wancom2
        description                             HA_HEARTBEAT2
        pri-utility-addr                        169.254.2.1
        sec-utility-addr                        169.254.2.2
        netmask                                 255.255.255.252
phy-interface
        name                                    s0p0
        operation-type                          Media
phy-interface
        name                                    s0p1
        operation-type                          Media
        port                                    1
phy-interface
        name                                    s1p0
        operation-type                          Media
        slot                                    1
phy-interface
        name                                    s1p1
        operation-type                          Media
        port                                    1
        slot                                    1
phy-interface
        name                                    wancom1
        port                                    1
        duplex-mode
        speed
        wancom-health-score                     8
```

```
phy-interface
        name                                    wancom2
        port                                    2
        duplex-mode
        speed
        wancom-health-score                     9
realm-config
        identifier                              Agent
        description                             Contact center agent facing realm
        network-interfaces                      s0p1:0
realm-config
        identifier                              Sema-clean
        network-interfaces                      s0p0:0
realm-config
        identifier                              Sema-dirty
        network-interfaces                      s1p0:0
realm-config
        identifier                              Customer
        description                             External customer facing realm
        network-interfaces                      s1p1:0
redundancy-config
        becoming-standby-time                   360000
        peer
                name                                    SBC1
                type                                    Primary
                destination
                        address                                 169.254.1.1:9090
                        network-interface                       wancom1:0
                destination
                        address                                 169.254.2.1:9090
                        network-interface                       wancom2:0
        peer
                name                                    SBC2
                type                                    Secondary
                destination
                        address                                 169.254.1.2:9090
                        network-interface                       wancom1:0
                destination
                        address                                 169.254.2.2:9090
                        network-interface                       wancom2:0
session-agent
        hostname                                10.232.50.211
        ip-address                              10.232.50.211
        realm-id                                Agent
        description                             Agent
session-agent
        hostname                                172.16.5.100
        ip-address                              172.16.5.100
        realm-id                                Sema-clean
        ping-method                             OPTIONS
        ping-interval                           30
session-agent
        hostname                                172.16.5.200
        ip-address                              172.16.5.200
        realm-id                                Sema-dirty
        ping-method                             OPTIONS
```

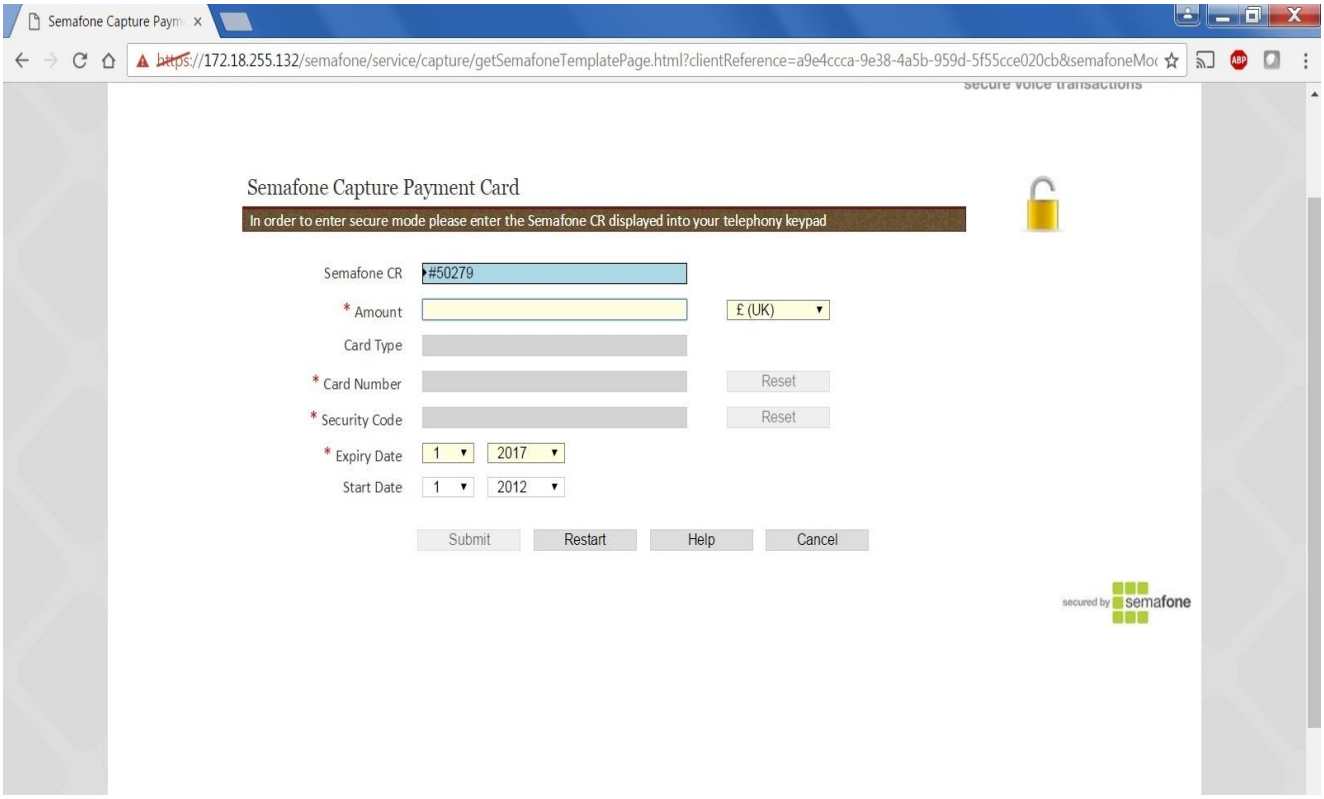
```
        ping-interval                           30
session-agent
        hostname                                192.160.2.150
        ip-address                              192.160.2.150
        realm-id                                Customer
        description                             Customer
sip-config
        home-realm-id                           Sema-clean
        registrar-domain                        *
        registrar-host                          *
        registrar-port                          5060
sip-interface
        realm-id                                Agent
        sip-port
                address                                 10.232.50.200
        rfc2833-mode                            preferred
sip-interface
        realm-id                                Sema-clean
        sip-port
                address                                 172.16.5.110
        rfc2833-mode                            dual
sip-interface
        realm-id                                Sema-dirty
        sip-port
                address                                 172.16.5.193
        in-manipulationid                       respondINFO
        rfc2833-mode                            dual
sip-interface
        realm-id                                Customer
        sip-port
                address                                 192.160.2.200
        rfc2833-mode                            preferred
sip-manipulation
        name                                    respondINFO
        description                             "Locally respond to INFO messages with Signal=E"
        header-rule
                name                                    storeINFOContent
                header-name                             Content-Type
                action                                  manipulate
                msg-type                                request
                methods                                 INFO
                element-rule
                        name                                    storeINFOContentBody
                        parameter-name                          application/dtmf-relay
                        type                                    mime
                        action                                  store
                        match-value                             Signal=E
        header-rule
                name                                    rejectINFO
                header-name                             Content-Type
                action                                  reject
                comparison-type                         boolean
                msg-type                                request
                methods                                 INFO
                match-value                             $storeINFOContent.$storeINFOContentBody
                new-value                               200:OK
```

```
sip-monitoring
        match-any-filter                        enabled
steering-pool
        ip-address                              10.232.50.200
        start-port                              50000
        end-port                                60000
        realm-id                                Agent
steering-pool
        ip-address                              172.16.5.110
        start-port                              40000
        end-port                                40100
        realm-id                                Sema-clean
steering-pool
        ip-address                              172.16.5.193
        start-port                              40000
        end-port                                45000
        realm-id                                Sema-dirty
steering-pool
        ip-address                              192.160.2.200
        start-port                              40000
        end-port                                50000
        realm-id                                Customer
system-config
        process-log-level                       DEBUG
        comm-monitor
                state                                   enabled
                monitor-collector
                        address                                 172.18.255.101
        default-gateway                         172.18.0.1
web-server-config
```

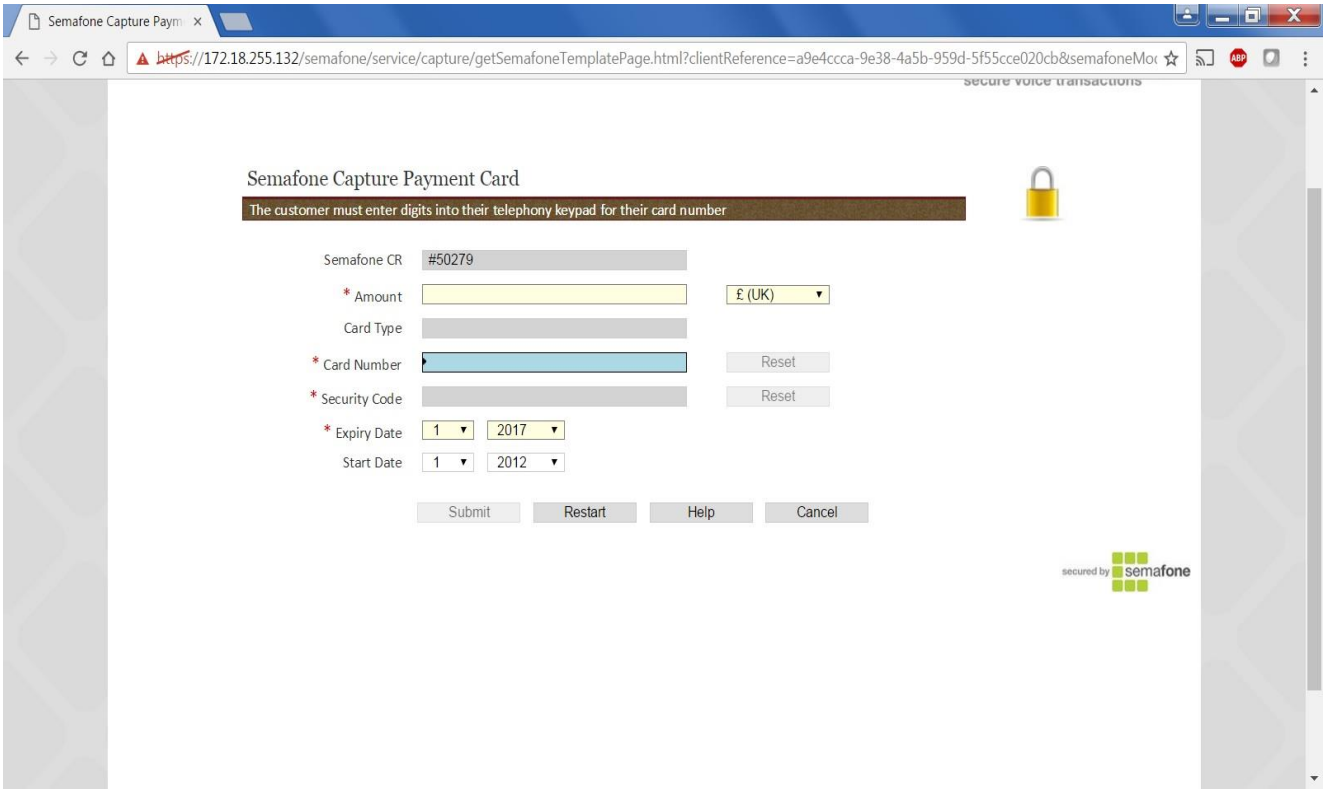
Screenshots from Semafone payment page

Following are the screenshots from Semafone payment page. The agent has access to this page through his desktop, when the customer who wants to make a payment calls; the agent presses the secure code generated on the page which triggers Semafone to go into Secure Mode. Then the customer enters the payment information and the agent can monitor and submit it when it's done.

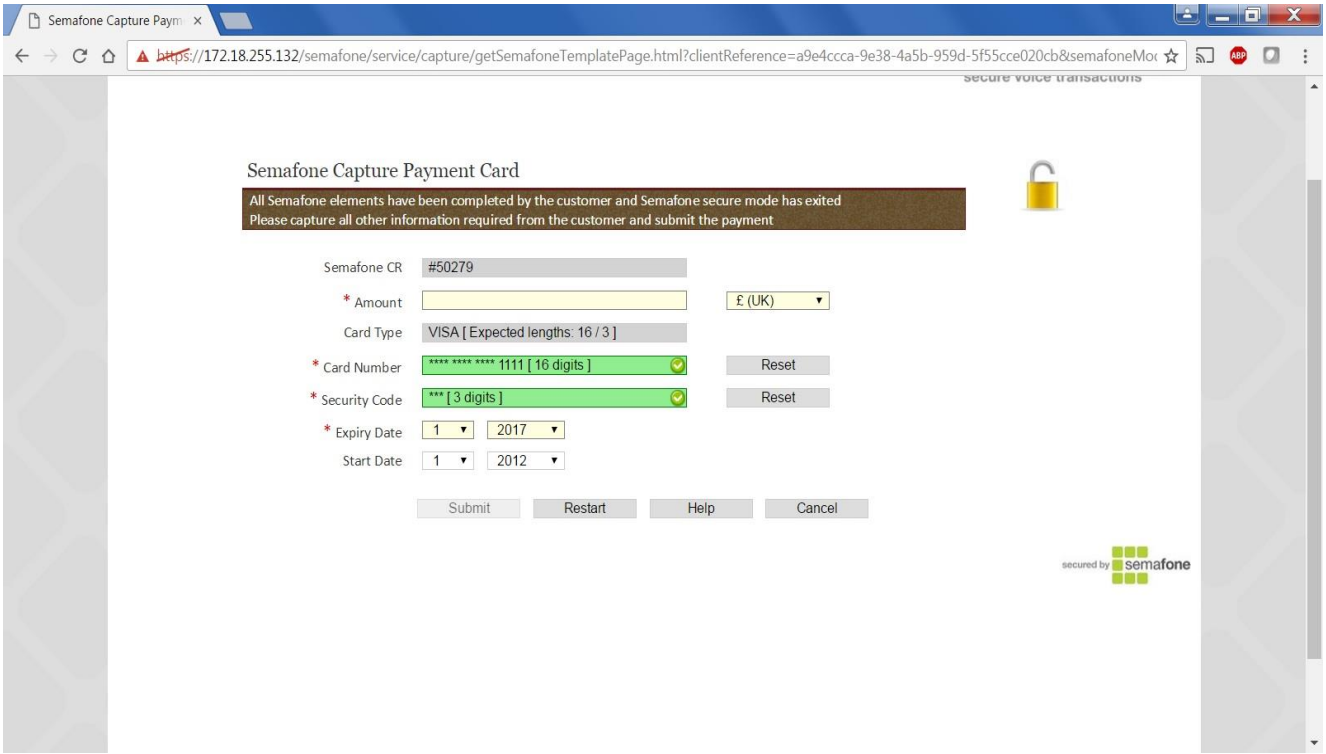
1) Agent enters the secure code on the phone which is generated on the payment page. #50279 in this case. The code is auto generated and is unique for every call.



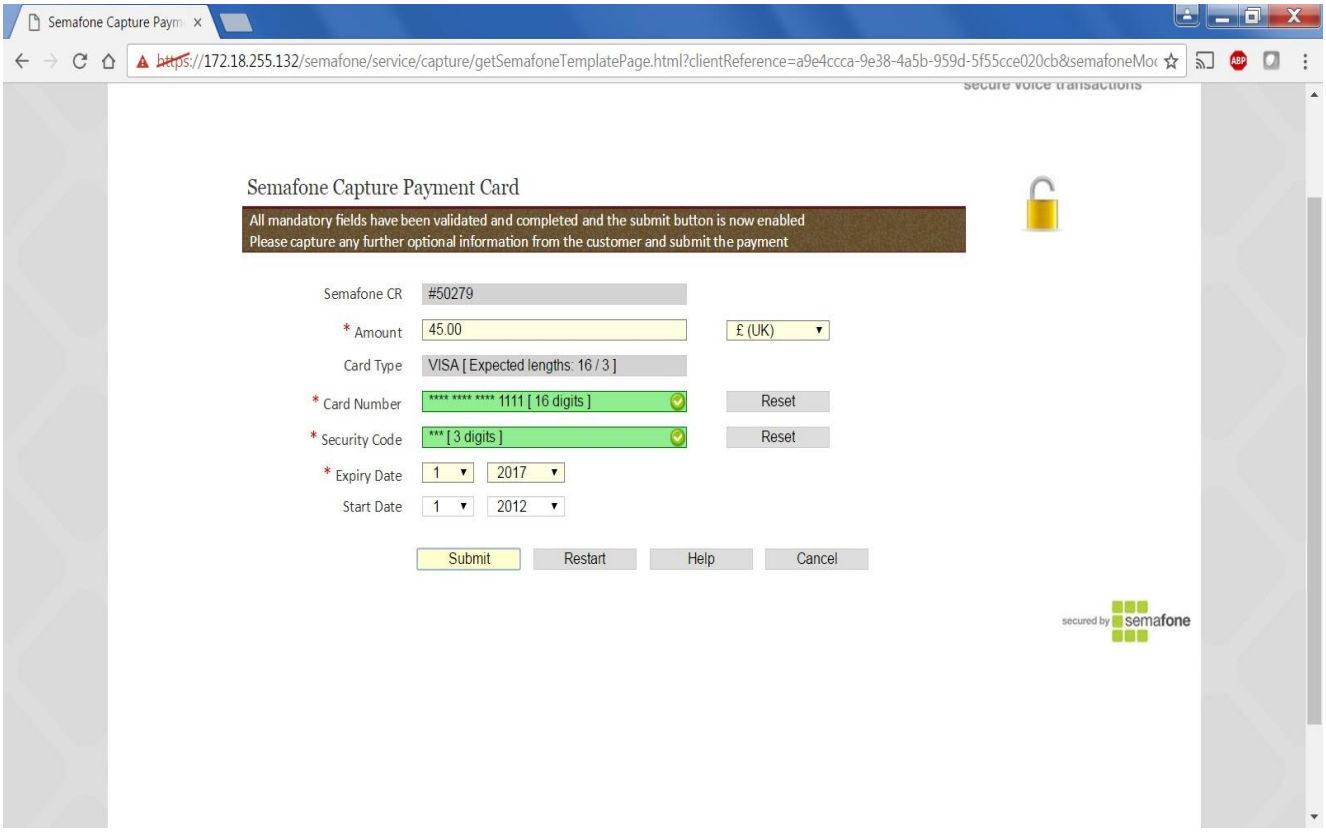
2) After the agent enters the CR, the lock symbol on the payment page changes from unlocked to locked.



3) The customer then enters the 16 digit credit card number followed by the 3 digit CVV. Note that the lock symbol changes back to unlocked after all the digits have been entered.



4) The agent then enters the payment amount and clicks on the Submit button to submit the payment.



Test Plan Executed

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

The codecs G729b, G711 u-law and G711 a-law have been tested as part of this certification for the following DTMF modes:

- Inband DTMF
- Outband/RFC2833 DTMF
- SIP INFO

Test Case no.	Codec/DTMF Format	Call Direction	DTMF Direction	Test outcome	Notes
1.1	G.729 Annex-B /RFC2833	Customer to Agent	Outbound/Inbound	Pass	
1.2	G.729 Annex-B /RFC2833	Agent to Customer	Outbound/Inbound	Pass	
1.3	G.729 Annex-B /SIP INFO	Customer to Agent	Outbound/Inbound	Pass	
1.4	G.729 Annex-B /SIP INFO	Agent to Customer	Outbound/Inbound	Pass	

Table 1 - Codec G.729 Annex-B

Test Case no.	Codec/DTMF Format	Call Direction	DTMF Direction	Test Outcome	Notes
2.1	G.711 A-LAW /inband	Customer to Agent	Outbound/Inbound	Pass	
2.2	G.711 A-LAW /inband	Agent to Customer	Outbound/Inbound	Pass	
2.3	G.711 A-LAW /RFC2833	Customer to Agent	Outbound/Inbound	Pass	
2.4	G.711 A-LAW /RFC2833	Agent to Customer	Outbound/Inbound	Pass	
2.5	G.711 A-LAW /SIP INFO	Customer to Agent	Outbound/Inbound	Pass	
2.6	G.711 A-LAW /SIP INFO	Agent to Customer	Outbound/Inbound	Pass	

Table 2 - Codec G.711 A-law

Test case no.	Codec/DTMF Format	Call Direction	DTMF Direction	Test Outcome	Notes
3.1	G.711 u-law /inband	Customer to Agent	Outbound/Inbound	Pass	-
3.2	G.711 u-law /inband	Agent to Customer	Outbound/Inbound	Pass	
3.3	G.711 u-law /RFC2833	Customer to Agent	Outbound/Inbound	Pass	
3.4	G.711 u-law /RFC2833	Agent to Customer	Outbound/Inbound	Pass	
3.5	G.711 u-law /SIP INFO	Customer to Agent	Outbound/Inbound	Pass	
3.6	G.711 u-law /SIP INFO	Agent to Customer	Outbound/Inbound	Pass	

Table 3 - Codec G.711 u-law

TroubleshootingTools

On the Oracle E-SBC

The Oracle 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 SBC Console:

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

Examining the log files

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

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 oraclesbc1FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

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

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle Enterprise Session Border Controller, and provides traces in a common log format for local viewing or for exporting to your PC. Please check the "Monitor and Trace" section (page 145) of the Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm

Telnet

Since we are working within an architecture which uses bound TCP listening ports for functionality, the simplest form of troubleshooting can be seeing if the devices are listening on a particular port, as well as confirming that the there is nothing blocking them such as firewalls.

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.

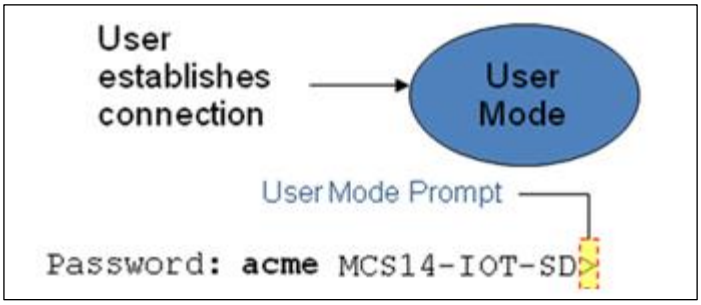
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

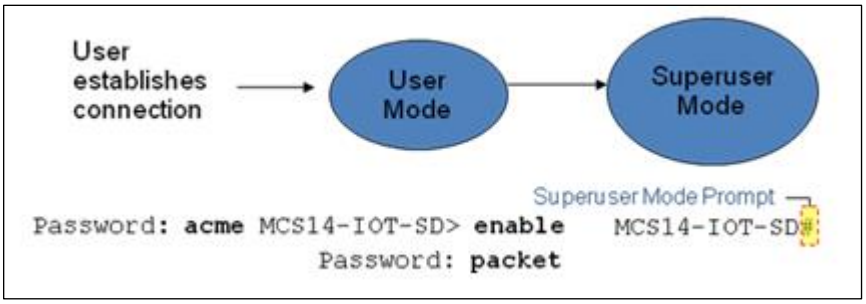
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

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

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



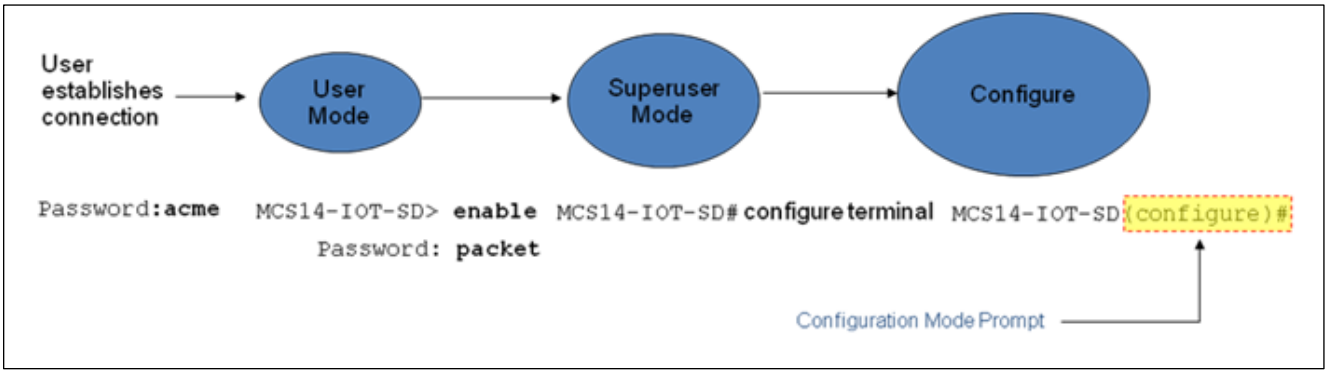
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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

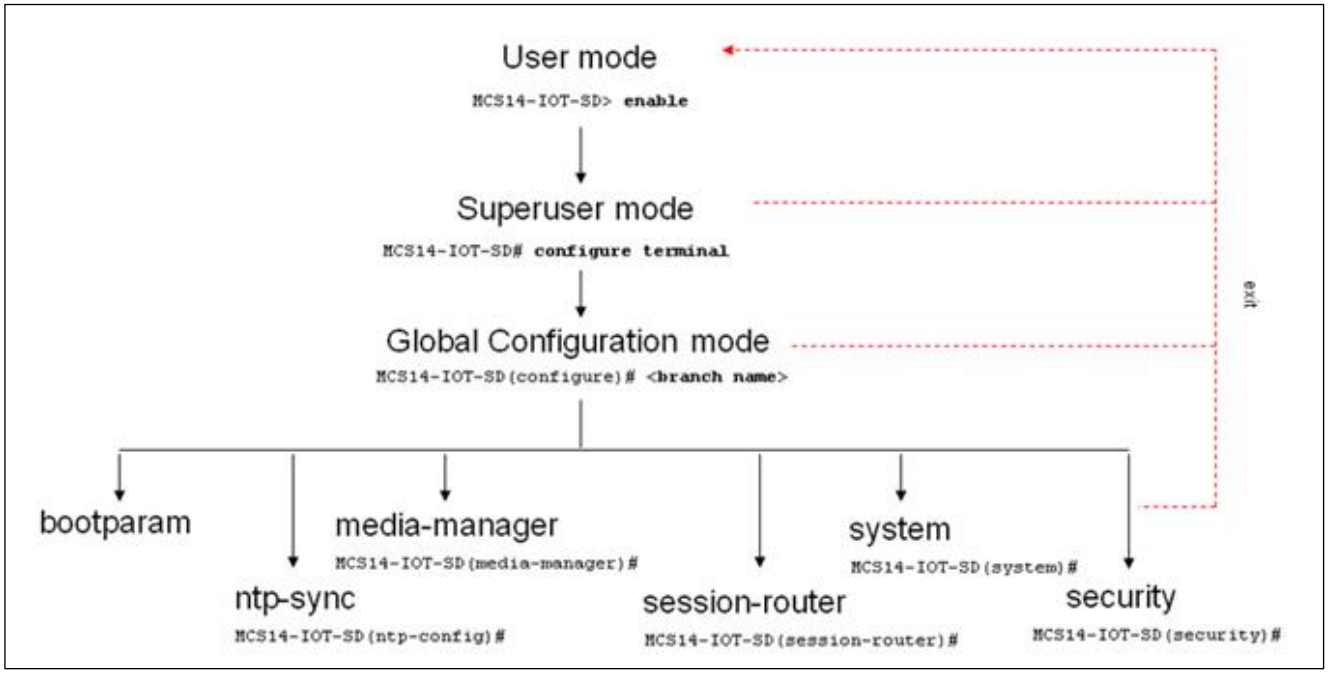
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, **oraclesbc1(configure)#**. To return to the Superuser mode, issue the **`exit`** command.



In the configuration mode, there are six configuration branches:

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



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

The bootparam branch provides access to SBC boot parameters. 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 SBC time and date.

The security branch provides access to security configuration.

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

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

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

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

Configuration Elements

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

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

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

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

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

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.

3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **show** command before issuing the **done** command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the **done** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the **exit** command to exit the selected element.

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

Editing an Element

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

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

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

Deleting an Element

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

To delete a single-instance element,

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

To delete a multiple-instance element,

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

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

Configuration Versions

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

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

Saving the Configuration

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

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

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

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

```
oraclesbc1 # save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbc1 #
```

Activating the Configuration

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

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

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


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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200