



ORACLE®

Oracle Enterprise Session Border Controller
and Cisco Unified Communications Manager
with SIP/TLS and RTP Trunking with the
Oracle Enterprise Operations Monitor

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	4
DOCUMENT OVERVIEW	4
INTRODUCTION	5
REQUIREMENTS.....	5
LAB CONFIGURATION	5
CAVEATS.....	7
PHASE 1 – CONFIGURING THE ORACLE ENTERPRISE SESSION BORDER CONTROLLER	8
IN SCOPE.....	8
OUT OF SCOPE	8
WHAT WILL YOU NEED.....	8
SBC – GETTING STARTED	8
Establish the serial connection and logging in the SBC.....	9
Initial Configuration – Assigning the Management Interface an IP Address.....	9
CONFIGURING THE ORACLE ENTERPRISE SBC (E-SBC)	10
High Availability (Local to a Particular Site)	10
Certificate-Records.....	10
Importing Trusted Certificates.....	10
Generating the SBC’s Certificate Signing Requests	11
Importing the SBC’s Signed Certificates	12
Local Policy.....	12
Media Manager.....	13
Media Security Policies.....	13
Network Interfaces.....	13
Physical Interfaces.....	13
Realm Configs	14
SDES Profile.....	14
Session Agents.....	14
Session Translation	14
SIP Config.....	15
SIP Interfaces.....	15

SIP Manipulations (Header Manipulation Rules – HMR)	15
Steering Pools	17
System Config	17
TLS Profile.....	17
Translation Rule	18
Web Server Config.....	18
Save, Activate, and Reboot	18
PHASE 2 – CONFIGURING THE ORACLE ENTERPRISE OPERATIONS MONITOR.....	19
IN SCOPE.....	19
OUT OF SCOPE	19
WHAT WILL YOU NEED.....	19
EOM – GETTING STARTED.....	19
CONFIGURING EOM TO DISPLAY ALL LEGS OF A CALL IN A SINGLE REPORT	20
PHASE 3 – CONFIGURING THE CISCO UNIFIED COMMUNICATIONS MANAGER (CUCM)	28
Generating a Certificate Signing Request (CSR) for CallManager	28
Importing the Certificate Authority (CA) Certificate.....	34
Importing the CallManager certificate signed by a CA	37
Configuring a SIP Trunk Security Profile	39
Creating a SIP Profile.....	45
Configuring a SIP Trunk.....	49
Creating a Route Pattern.....	54
Setting the cluster to Mixed Mode.....	61
TEST PLANS & RESULTS	64
TEST PLAN	64
TROUBLESHOOTING TOOLS	64
WIRESHARK.....	64
ON THE ORACLE E-SBC.....	64
Examining the log files.....	65
Through the Web GUI.....	65
ORACLE ENTERPRISE OPERATIONS MONITOR (EOM).....	65
APPENDIX A	66
ACCESSING THE ACLI.....	66
ACLI BASICS	66
CONFIGURATION ELEMENTS	68
CREATING AN ELEMENT.....	68
EDITING AN ELEMENT.....	68
DELETING AN ELEMENT.....	69
CONFIGURATION VERSIONS.....	69
SAVING THE CONFIGURATION	69
ACTIVATING THE CONFIGURATION	70



Intended Audience

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

Document Overview

This technical application note documents the implementation of the Oracle Enterprise Session Border Controller (E-SBC) trunk-side between the Cisco Unified Communications Manager (CUCM) and a Service Provider network.

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

Introduction

Enterprise Session Border Controller Overview

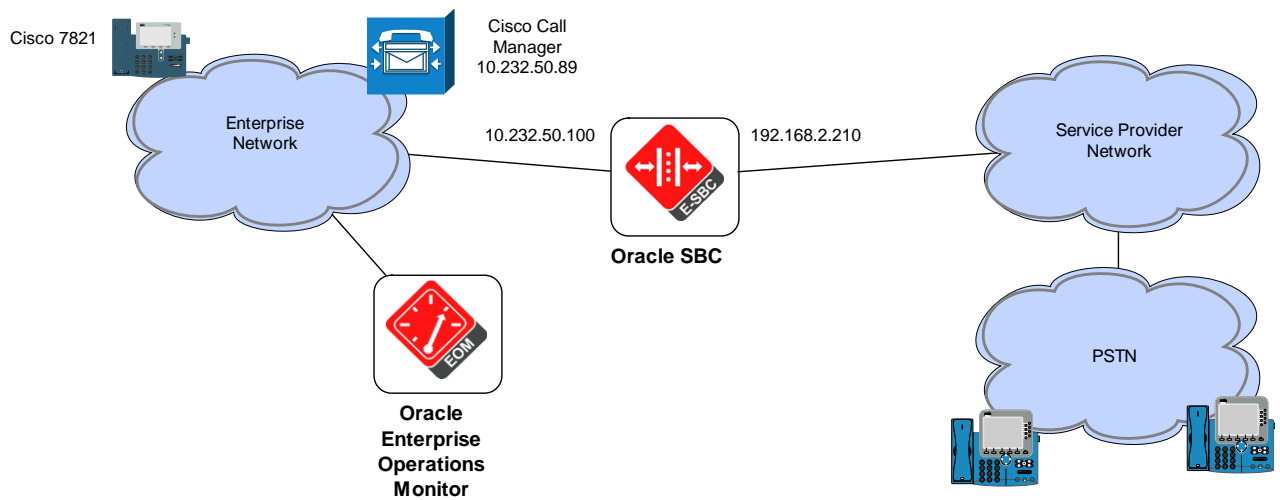
The Oracle Enterprise Session Border Controller (E-SBC) is an enterprise-class signaling component designed to simplify communications networks. It connects disparate IP communications networks while mitigating security threats, curing interoperability problems and ensuring reliability.

Requirements

- Oracle Enterprise Session Border Controller ECZ7.3.0 MR-1 Patch 1
- Oracle Enterprise Operations Monitor 3.3.90.0.0
- Cisco CUCM version 10.5.2.10000-5

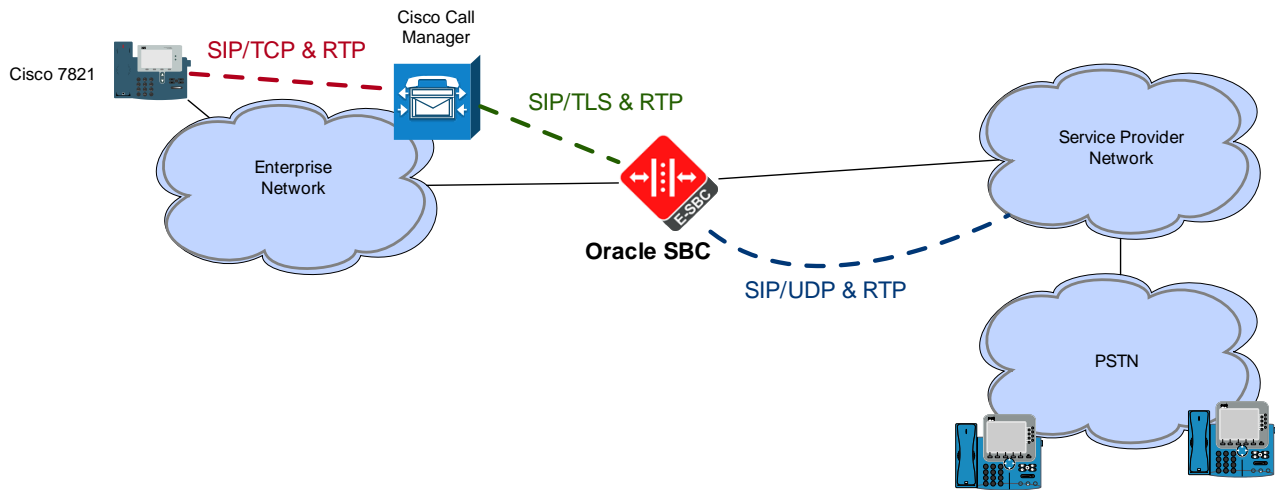
Lab Configuration

The following diagram illustrates the lab environment used for testing.



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

The communication between the Cisco phone and CUCM is SIP-over-TCP and RTP. It is outside the scope of this document to detail the configuration for this area. The communication between CUCM and the Oracle SBC is SIP-over-TLS and RTP, and the Oracle SBC converts this to SIP-over-UDP and RTP going to the Service Provider network. It should be possible to use all Secure RTP (SRTP) on the trunk side, but this was not tested.





Caveats

- This configuration includes replacing CUCM's self-signed certificate with one signed by a third-party Certificate Authority (CA). Since CUCM uses this certificate to sign the phone configuration files, no changes to the config files is possible without also importing the CA certificate onto the phones. Importing the CA certificate onto the phones was not performed during this testing.
- The Oracle SBC supports converting between Secure RTP (SRTP) and RTP, and an example configuration is given in this document even though it was not tested.

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

- Phase 1 – Configuring the Oracle E-SBC
- Phase 2 – Configuring the Oracle EOM
- Phase 3 – Configuring the Cisco Unified Communications Manager (CUCM) 10.5

Phase 1 – Configuring the Oracle Enterprise Session Border Controller

In this section we describe the steps for configuring Oracle Enterprise SBC (E-SBC) for trunking with the Cisco Unified Communication Manager (CUCM).

In Scope

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

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

Out of Scope

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

What will you need

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

SBC – Getting Started

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

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

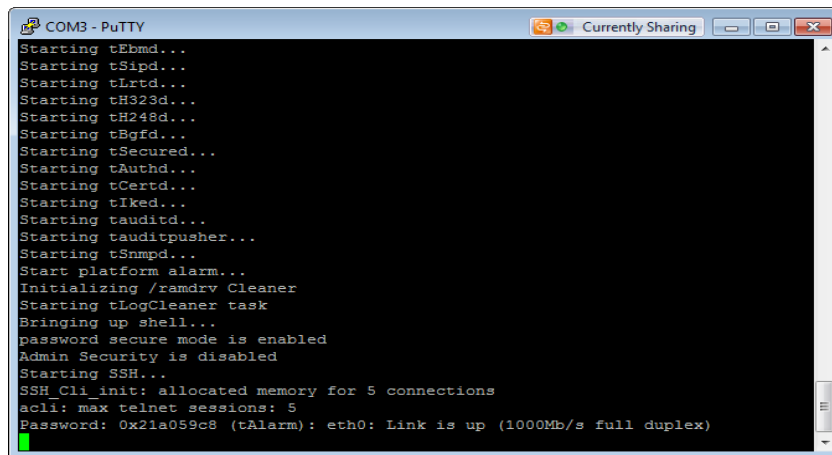
All commands are in bold, such as **configure terminal**; parameters in bold red such as **oraclesbc1** are parameters which are specific to an individual deployment. Only non-default parameters are shown. **Note:** The CLI is case sensitive.

Establish the serial connection and logging in the SBC

Confirm the SBC is powered off and connect one end of a straight-through Ethernet cable to the console port on the SBC and the other end to the console adapter that ships with the SBC, connect the console adapter (a DB9 adapter) to the DB9 port on a workstation, running a terminal emulator application such as PuTTY. Start the terminal emulation application using the following settings:

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

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



```
COM3 - PuTTY
Starting tEhmd...
Starting tSipd...
Starting tLtd...
Starting tH323d...
Starting tH248d...
Starting tBgf...
Starting tSecured...
Starting tAuth...
Starting tCertd...
Starting tKed...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Start platform alarm...
Initializing /ramdrv Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH_Cli_init: allocated memory for 5 connections
acli: max telnet sessions: 5
Password: 0x21a059c8 (tAlarm): eth0: Link is up (1000Mb/s full duplex)
```

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

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

You are now in the global configuration mode.

Initial Configuration – Assigning the Management Interface an IP Address

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

oraclesbc1# configure terminal --> bootparam

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

```
oraclesbc1(configure)# bootparam

'.' = clear field: '-' = go to previous field: α = quit

Boot File      : /boot/ nnECZ730m1p1.64.bz
IP Address     : 192.168.79.44
VLAN          :
Netmask       : 255.255.255.224
```

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

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

Configuring the Oracle Enterprise SBC (E-SBC)

The following section walks you through configuring the Oracle Enterprise SBC required to work with CUCM. It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

High Availability (Local to a Particular Site)

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

Certificate-Records

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

```
certificate-record
  name          CAcert
  locality      Bedford
  organization   Oracle
  common-name    Oracle PE Lab CA
  key-size      2048
certificate-record
  name          SBCcert
  locality      Bedford
  organization   Oracle
  unit          PE
  common-name    trunking-sbc.pe.oracle.com
  key-size      2048
```

Importing Trusted Certificates

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

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

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

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

IMPORTANT:

Please enter the certificate in the PEM format.

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

```
-----BEGIN CERTIFICATE-----
```

```
MIIlCojCCAgugAwIBAgIBADANBgkqhkiG9w0BAQUFADBvMRUwEwYDVQQDEwxxOTlu
MjAwLjEuMTEwEzARBgNVBAsTCkNvbnRyYWN0b3IxDDAKBgNVBAsTA1BLSTEMMAoG
A1UECXMDRG9EMRgWfGyYDVQQKEw9VLIUuIEdvdmVybml1bnQxMzA1BjgNVBAYTAIVT
MB4XDTA5MDYwMTIxMzExMl0XDTEwMDYwMTIxMzExMl0wZEVMBMGA1UEAxMMMTky
LjllwMC4xLjEwEzMRMwEQYDVQQLEwpDb250cmFjdG9yMQwwCgYDVQQLEwNQS0kxDDAK
BgNVBAsTA0RvRDEYMBYGA1UEChMPVS5TLiBhb3Zlcm5tZW50MQswCQYDVQQGEwJV
UzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygvCYGGWd+zXqo/2waPWBQbU
uLYFD0DCuA+AhemNR/ueiBMnpaBfD6eJwYaVj9jfwTC/EdO3gLuqWsnscgCRKgc
oQcWUBH/EaCFFKIEPnhU8znAr1otr+5I4PvFUZMleODJ51R4Um2Q3XIRIJrhGNOC
k42juxhYe1Ay2m6qTcECAwEAAaNOMEwwCQYDVR0TBAlwADAQBgNVHSUBAf8EFjAU
BggrBgEFBQcDAQYIKwYBBQUHAWkwHQYDVR0OBBYEFHqy2karD38Xp/Qje2ROAYjl
6SfsMA0GCSqSIlb3DQEBBQUAA4GBAFkNGCLXKI47vA+8p7vbpdmDhC8iZK2dP1b4
5WpflOvQBF/qZg5bj/j8lydU4cXpl9mi9Wt0gxc6DtWZuRfvs5n8Kq8q4juPGjMZ
b/pp5D5++vDe1LlaylrxzQbCZSKKJ8CkixYY4NHk6oAyHMz9OqjVTO1GWS7MZdLp
Sy+Q9Ma3
```

```
-----END CERTIFICATE-----; ← Note the semi-colon that was entered after the certificate
```

Certificate imported successfully....

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

```
oraclesbc1# save
```

checking configuration

Save-Config received, processing.

waiting for request to finish

Request to 'SAVE-CONFIG' has Finished,

Save complete

Currently active and saved configurations do not match!

To sync & activate, run 'activate-config' or 'reboot activate'.

```
oraclesbc1# activate-config
```

Activate-Config received, processing.

waiting for request to finish

Request to 'ACTIVATE-CONFIG' has Finished,

Activate Complete

```
oraclesbc1#
```

Generating the SBC's Certificate Signing Requests

The SBC only needs one certificate with the Common Name set to a Fully Qualified Domain Name (FQDN). To generate a certificate signing request, the certificate must be configured as a certificate-record with the appropriate fields (as dictated by the

signing CA's policies), followed by a save/activate. Each certificate signing request can then be generated using the "generate-certificate-request <certificate-record-name>". The certificate signing request can then be given to the CA to be signed. Here is an example generation of a certificate signing request:

generate-certificate-request ExampleSbcCertA

Generating Certificate Signing Request. This can take several minutes....

```
-----BEGIN CERTIFICATE REQUEST-----
MIIByTCCATICAQAwwXjELMAKGA1UEBhMCMVVMx CzAJBgNVBAgTAK1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEXMBUGA1UEAxMOMMTky
LjE2OC4xMy4xMTMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANoAWTk8tHzE
tbICL88CFwx9s9soqbKr0u+ZSJQEKsV0OUMtPX60X5+Z94TORp1waZMcSTSHktrM
OrUsF8j9OV/5YvcJFWvxvMXOpivdO9Tbd7M44776P41weI BRXNBv7aWv2qzc4gUx
IFXRcf4xBnyZIIxLxEwO68ezZxB3y8EUNAgMBAAGGKzApBgNVHQ8xIhMgZGlnaXRh
bFNpZ25hdHVyZSxrZXIFbmNpcGhlcmlbnQwDQYJKoZIhvcNAQEFBQADgYEAcsZH
6nig6A2GgAnCTUTjraJH/bMHoFQkeXOWcmUf84u6VKyV/9EDhIE/hdjG5/32KIXP
d6zQ7J9GeanvrkSqa757rl2uqbRR/cQIWPNGAG4TocNwdkZznGYm9Du4qPH4ceSh
stD/bBql63NjkSKrQXwpB6VZYfcATH6X++7VRco=
-----END CERTIFICATE REQUEST-----
```

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

Then save and activate the configuration; the private key will be stored.

Copy and paste the request, including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" into a text file and give the file to the CA.

Importing the SBC's Signed Certificates

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

Managing Certificate Expirations to Avoid Service Disruptions

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

Local Policy

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

```
local-policy
  from-address          *
  to-address            *
  source-realm          cisco-core
  policy-attribute
    next-hop            192.168.2.60
    realm               trunk
local-policy
  from-address          *
  to-address            *
  source-realm          trunk
  policy-attribute
    next-hop            10.232.50.89
    realm               cisco-core
```

Media Manager

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

Media Security Policies

Path: `configure terminal > security > media-security > media-sec-policy`

```
media-sec-policy
  name                               rtp
media-sec-policy NOTE THIS IS GIVEN AS AN EXAMPLE ONLY. SRTP WAS NOT TESTED.
  name                               srtp
  inbound
    profile                          sdes-profile
    mode                             srtp
    protocol                         sdes
  outbound
    profile                          sdes-profile
    mode                             srtp
    protocol                         sdes
```

Network Interfaces

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

```
network-interface
  name                               s0p0
  ip-address                        192.168.2.210
  netmask                          255.255.255.0
  gateway                          192.168.2.200
  hip-ip-list                      192.168.2.210
  icmp-address                    192.168.2.210
network-interface
  name                               slp0
  ip-address                        10.232.50.100
  netmask                          255.255.255.0
  gateway                          10.232.50.86
  hip-ip-list                      10.232.50.100
  icmp-address                    10.232.50.100
```

Physical Interfaces

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

```
phy-interface
  name                               s0p0
  operation-type                     Media
phy-interface
  name                               slp0
  operation-type                     Media
  slot                               1
```

Realm Configs

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

```
realm-config
  identifier                cisco-core
  network-interfaces        slp0:0
  media-sec-policy          rtp <- Change to srtp to enable
SRTP. Note that SRTP was not tested.
realm-config
  identifier                trunk
  network-interfaces        s0p0:0
  media-sec-policy          rtp
```

SDES Profile

Path: `configure terminal > security > media-security > sdes-profile`

NOTE: This is only required for SRTP, which was not tested.

```
sdes-profile
  name                      sdes-profile
  crypto-list                AES_CM_128_HMAC_SHA1_32
```

Session Agents

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

```
session-agent
  hostname                 10.232.50.89
  ip-address               10.232.50.89
  port                      5061
  transport-method          StaticTLS
  realm-id                  cisco-core
  description                Cisco CUCM
  ping-method                OPTIONS;hops=0
  ping-interval              30
  out-translationid         stripone
session-agent
  hostname                 192.168.2.60
  ip-address               192.168.2.60
  realm-id                  trunk
  description                SIP Trunk
  ping-method                OPTIONS;hops=0
  ping-interval              30
```

Session Translation

Path: `configure terminal > session-router > session-translation`

```

session-translation
  id                               stripone
  rules-calling                    stripone
  rules-called                     stripone

```

SIP Config

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

```

sip-config
  home-realm-id                    cisco-core
  options                          max-udp-length=0

```

SIP Interfaces

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

```

sip-interface
  realm-id                          cisco-core
  sip-port
    address                         10.232.50.100
    port                             5061
    transport-protocol              TLS
    tls-profile                      TlsProfile
    allow-anonymous                 agents-only
  out-manipulationid                NAT_IP
sip-interface
  realm-id                          trunk
  sip-port
    address                         192.168.2.210
    allow-anonymous                 agents-only
  out-manipulationid                NAT_IP

```

SIP Manipulations (Header Manipulation Rules – HMR)

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

```

sip-manipulation
  name                              NAT_IP
  header-rule
    name                             NatFrom
    header-name                       From
    action                            manipulate
    msg-type                          request
    element-rule
      name                             NatFromIp
      type                             uri-host
      action                            replace
      new-value                         $LOCAL_IP
  header-rule
    name                              NatTo

```

header-name	To
action	manipulate
msg-type	request
element-rule	
name	NatToIp
type	uri-host
action	replace
new-value	\$REMOTE_IP

Steering Pools

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

steering-pool		
ip-address		10.232.50.100
start-port		49152
end-port		65535
realm-id		cisco-core
steering-pool		
ip-address		192.168.2.210
start-port		49152
end-port		65535
realm-id		trunk

System Config

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

system-config		
description		Oracle 4600 SBC for Cisco Trunk-
Side Testing		
process-log-level		DEBUG
NOTE: This should be changed to NOTICE after intial testing for performance reasons		
comm-monitor		
state		enabled
monitor-collector		
address		172.18.255.101
NOTE: This is the IP address of the Oracle Enterprise Operations Monitor (EOM).		
default-gateway		192.168.79.33
source-routing		enabled

TLS Profile

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

tls-profile		
name		TlsProfile
end-entity-certificate		SBCcert
trusted-ca-certificates		CAcert
mutual-authenticate		enabled
tls-version		tlsv1

Translation Rule

Path: **configure terminal > session-router > translation-rule**

```
translation-rules
  id                stripone
  type              delete
  delete-string     1
```

Web Server Config

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

```
web-server-config
  state             enabled
```

Save, Activate, and Reboot

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

```
oraclesbcl# 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'.
oraclesbcl# 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
oraclesbcl# reboot force
```

The E-SBC configuration is now complete.

Phase 2 – Configuring the Oracle Enterprise Operations Monitor

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

In Scope

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

Out of Scope

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

What will you need

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

EOM – Getting Started

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

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

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

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

The screenshot shows the Oracle Communications Operations Monitor (EOM) interface. The top right corner displays the user 'admin' and a dropdown menu with the following options: My Profile, Settings (circled in red), My Home, About the product, Help, Setup, and Logout. The main dashboard contains several widgets: 'Active calls' (line graph), 'Registered users' (line graph), 'Recent calls' (table), and 'User Device Distribution' (pie chart).

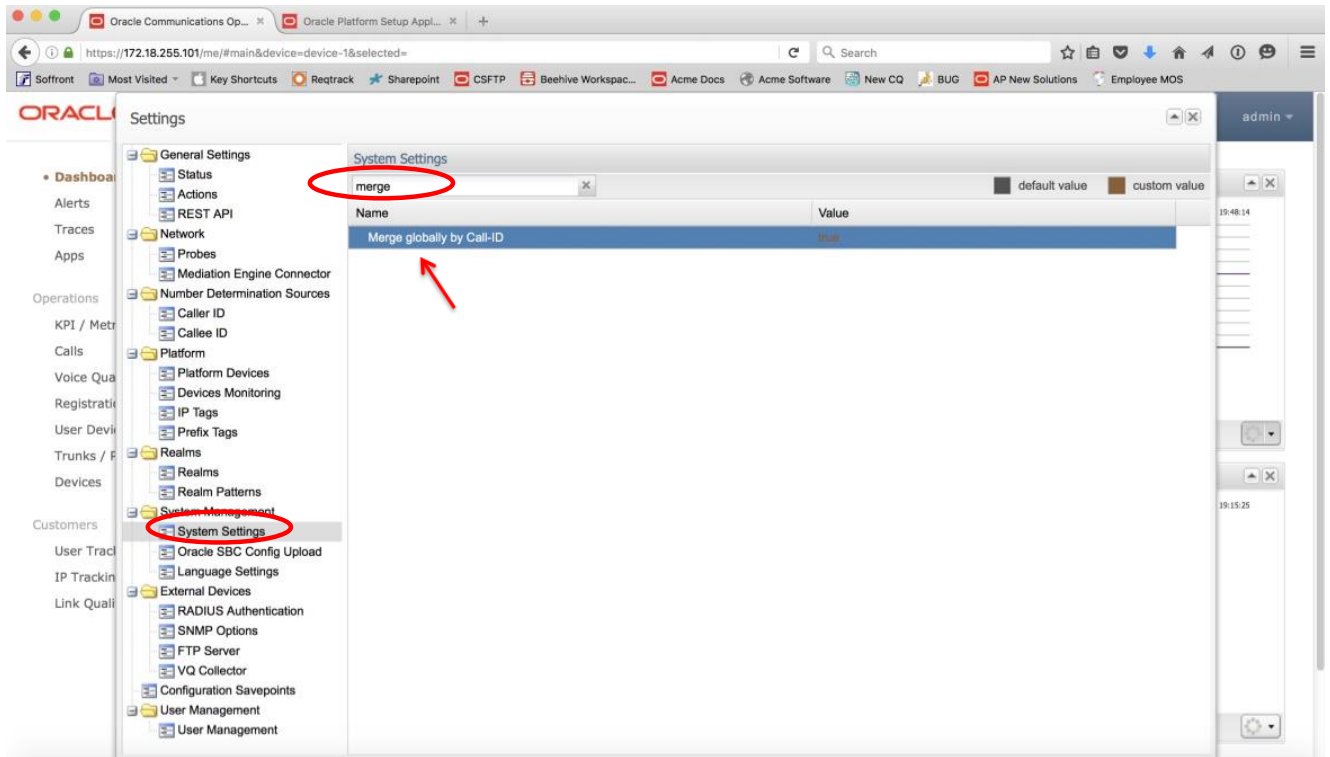
Caller	Callee	Call time	Seg...
7322162709	7322162720	6'368ms	4
7322162709	7322162720	8'551ms	2
7322162709	7322162720	8'544ms	2
7322162709	7322162720	5'568ms	4

User Device Distribution (2016-04-05 19:15:25):

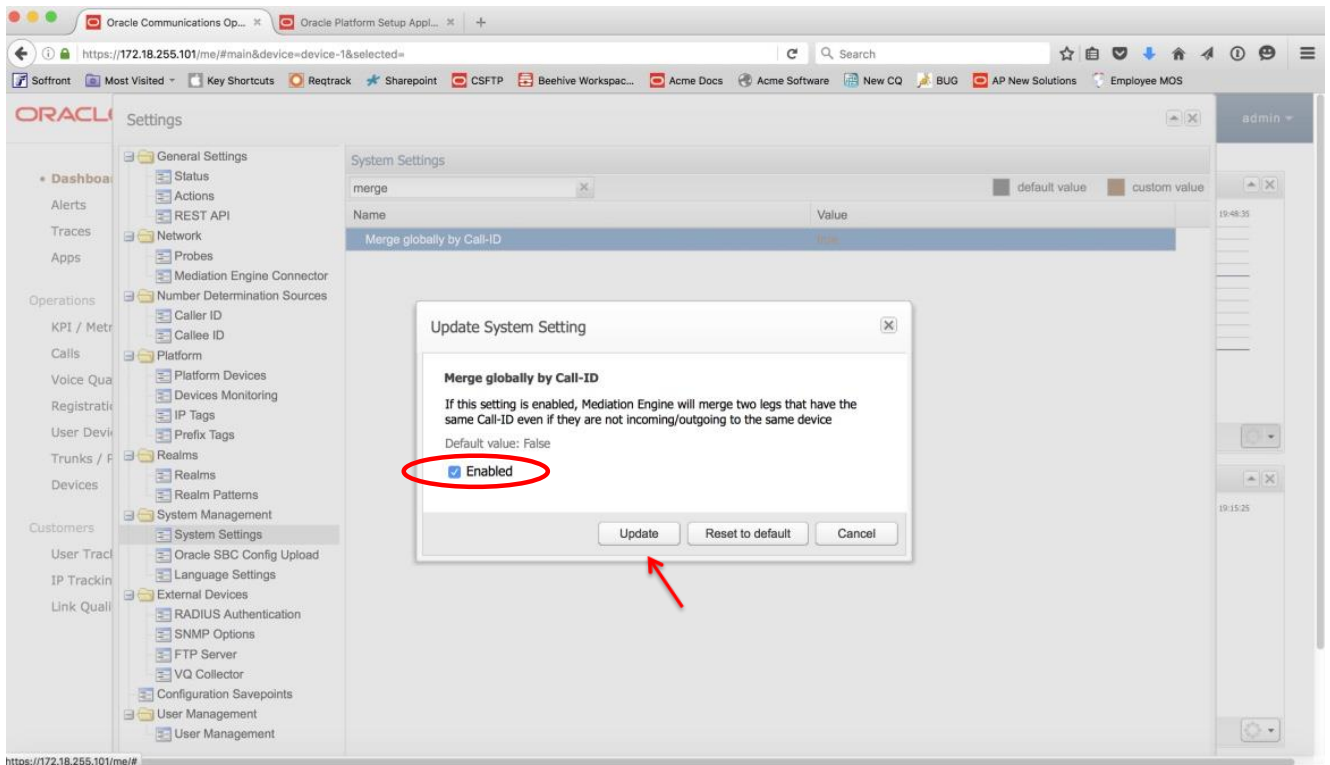
- Cisco-CP9971/9.4.2 (16.7%)
- Cisco-CP7821/10.2.1 (83.3%)

User devices (12 registrations on 2 devices)

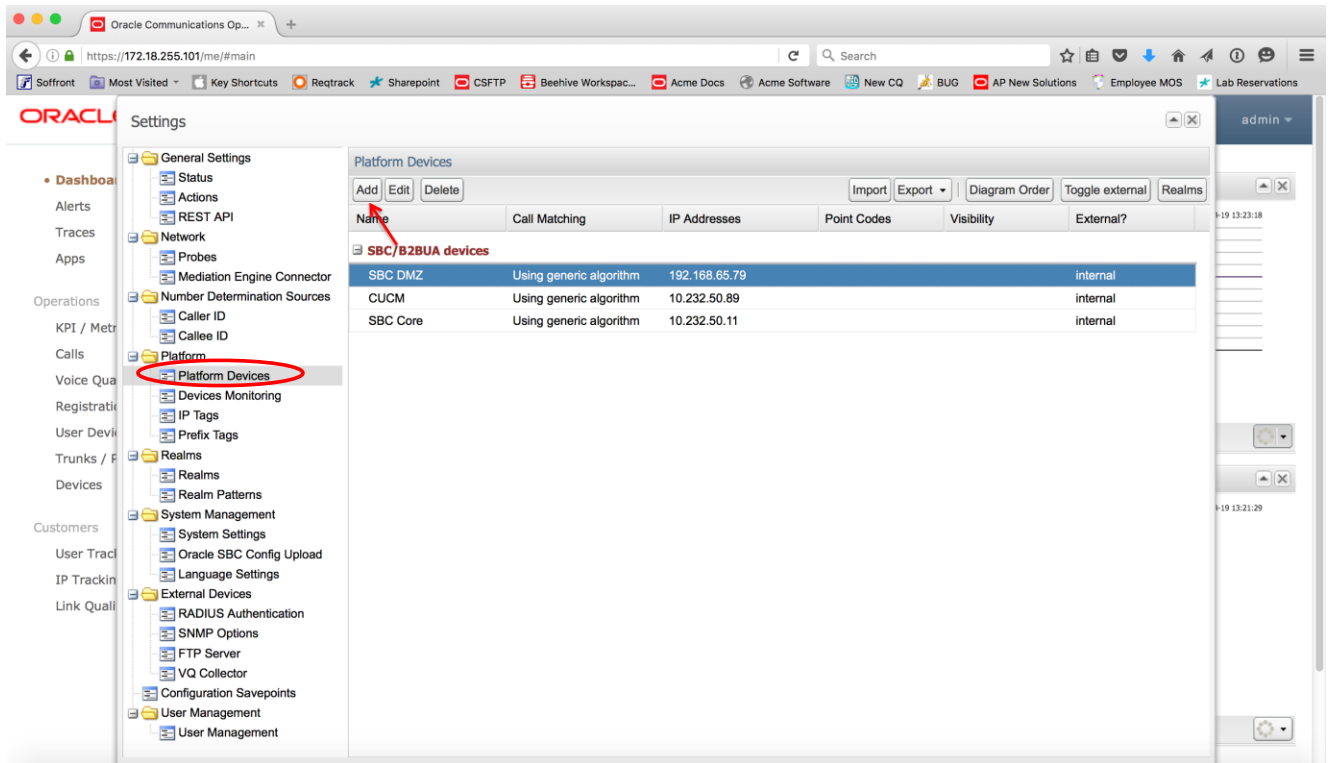
2. Under System Management select System Settings and search for “merge”. Double click on “Merge globally by Call-ID”.



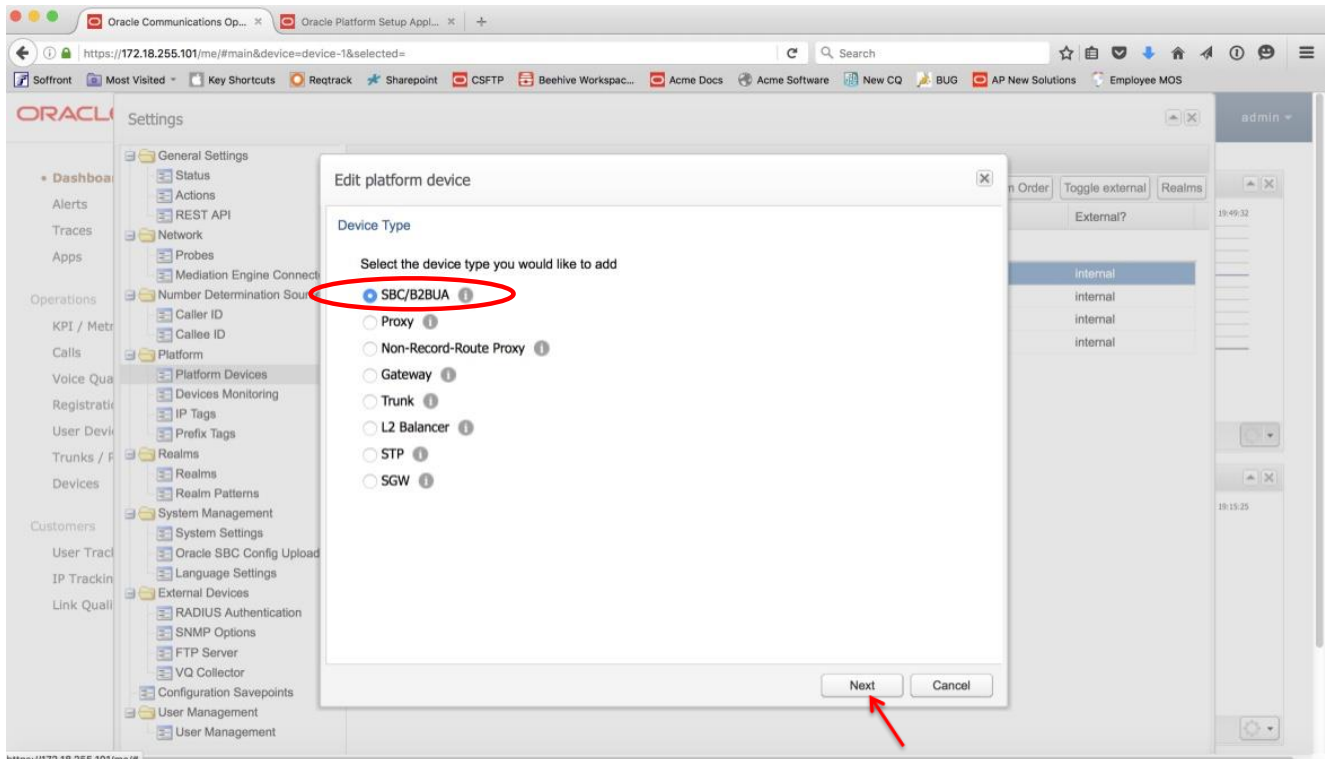
3. Click on the Enabled check box and click Update.



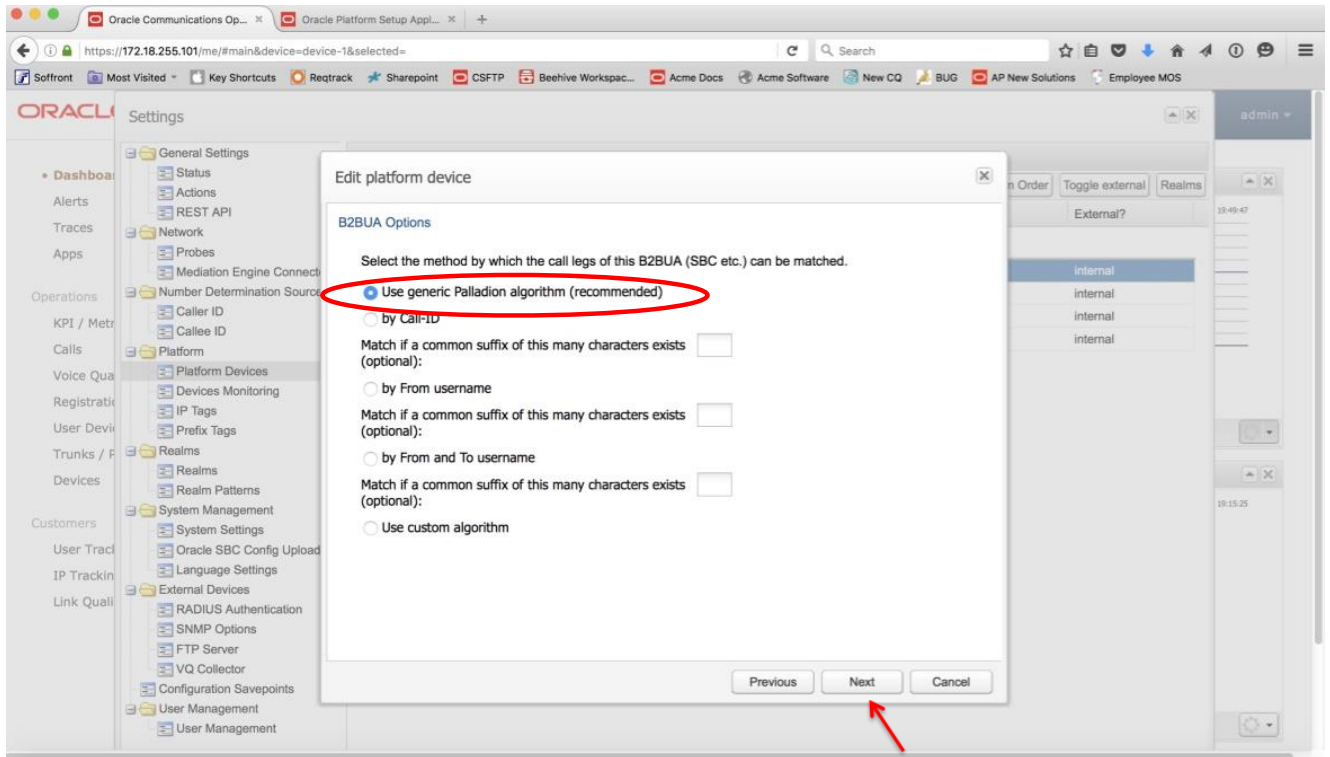
4. Under Platform select Platform Devices. Click Add (or Edit if you've already added a device).



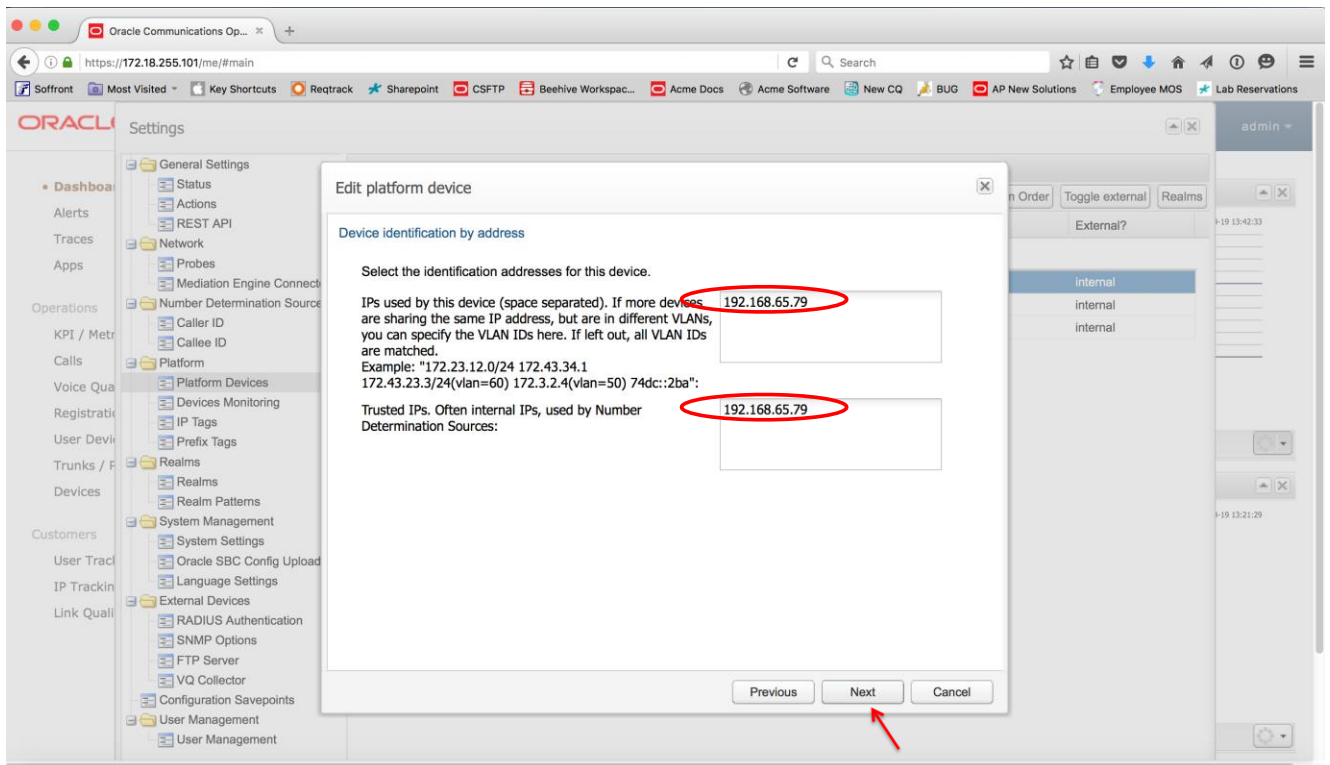
5. Select the SBC/B2BUA radio button regardless of the type of device you're adding, then click Next.



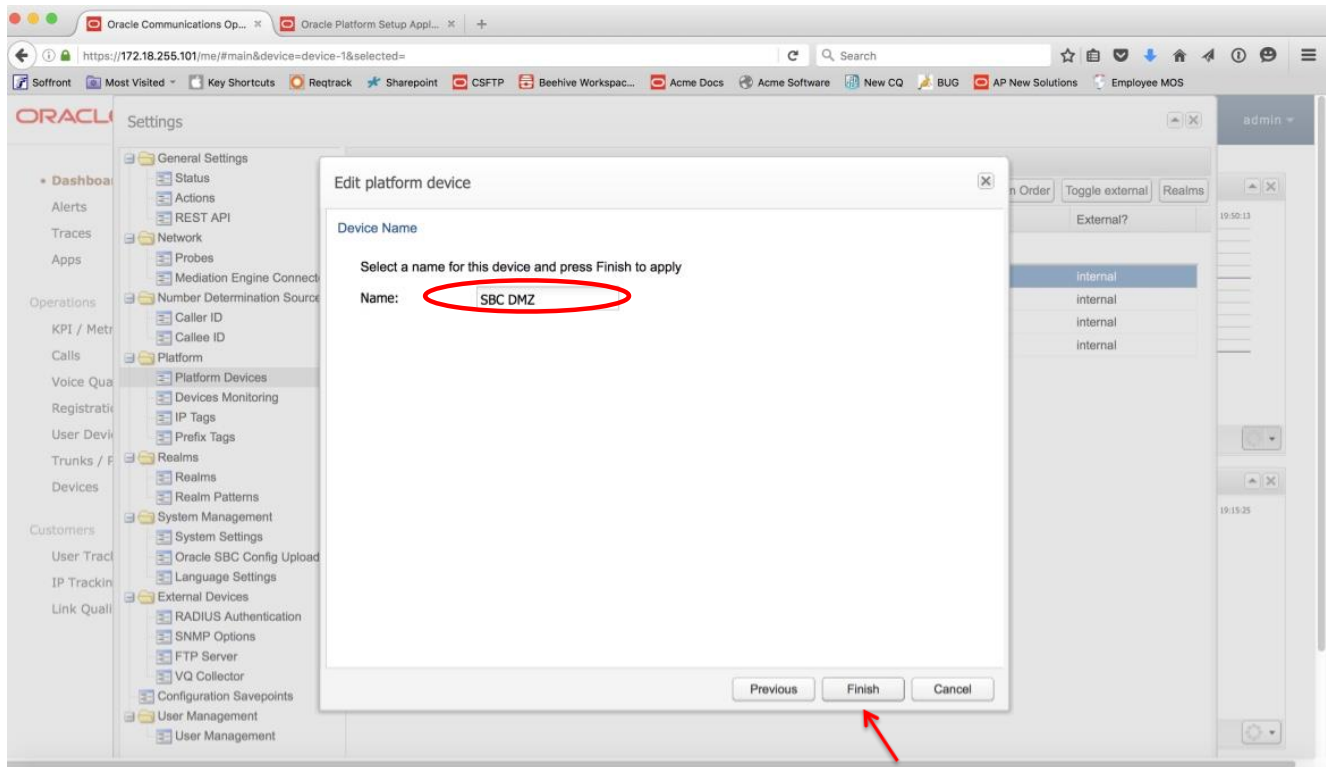
6. Click on the "Use generic Palladion algorithm (recommended)" radio button, then click Next.



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



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



9. Repeat for all other devices in the call flow. Enter each side of the SBC (inside and outside) separately.

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

The screenshot shows the Oracle Communications Operations Monitor dashboard. The 'Recent calls' table is visible with the following data:

Caller	Callee	Call time	Seg
+16175436463	6132606021	1'23"	2
+16175436463	6132606021	58"	2
+16175436463	6132606021	58"	2
6132606021	96175436463	8'366ms	2
6132606021	96175436463	14"	2
6132606021	96175436463	0'0ms	2

The 'Auto Refresh' dropdown menu is open, showing options: Off, 2 Seconds (selected), 5 Seconds, 10 Seconds, 30 Seconds, and 60 Seconds.

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

The screenshot shows the Oracle Communications Operations Monitor dashboard. The 'Recent calls' table is visible with the following data:

Caller	Callee	Call time	Seg...
7322162709	7322162720	6'366ms	4
7322162709	7322162720	8'551ms	2
7322162709	7322162720	8'544ms	2
7322162709	7322162720	5'568ms	4

A red arrow points to the first row of the table, which has 4 segments.

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

ORACLE

Call Report

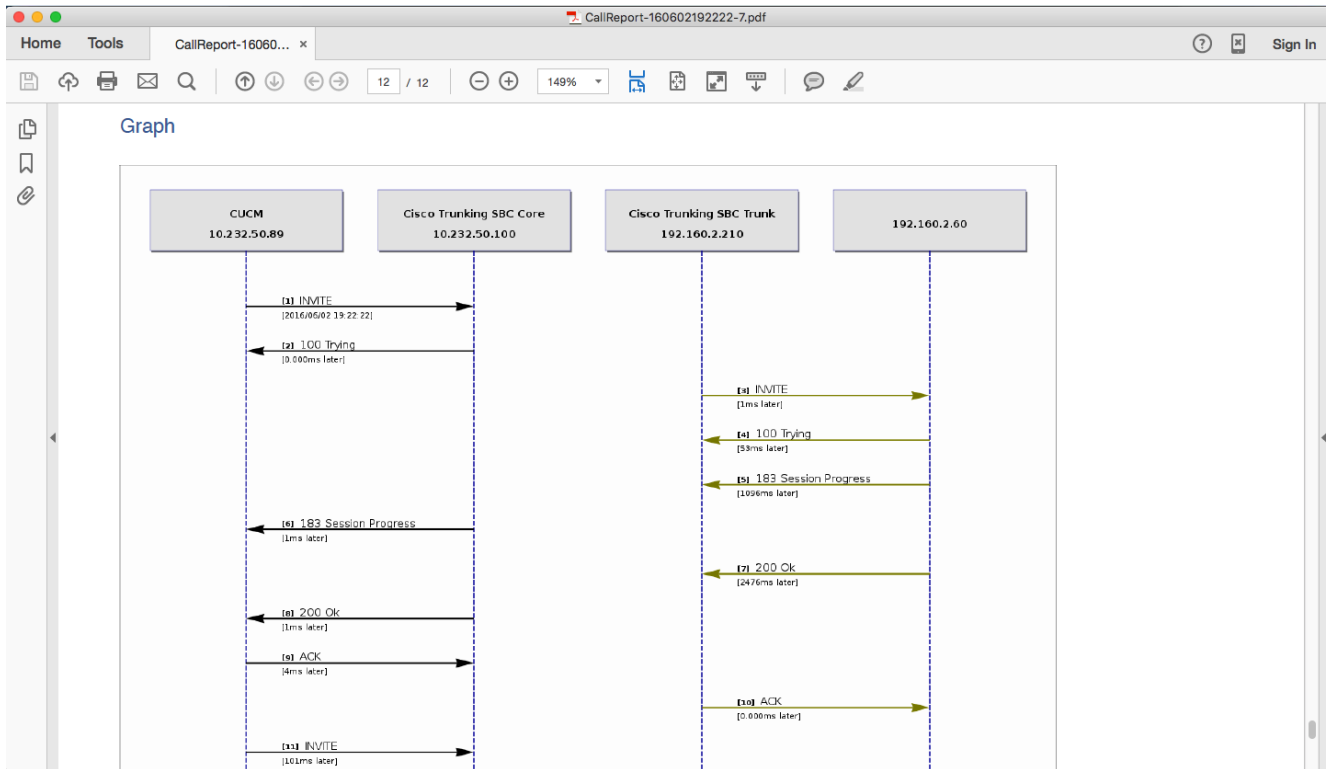
Call Information

Call:	Caller: 7814437285 Callee: 19123037947	Setup start time: 2016/06/02 19:22:22 Ringling time: 3631	Status: Finished
Segment 1:	10.232.50.89:52247 -> 10.232.50.100:5061 Call-ID: becd0e00-75018675-b61d-5932e80a@10.232.50.89 Caller uri: sip:7814437285@10.232.50.89 Callee uri: sip:19123037947@10.232.50.100	From tag: 160250-00b97701-5e47-02c7-c4f0-73777b880ae3-18960193 Last response code: 200 Caller device: Cisco-CUCM10.5	Status: Finished
Segment 2:	192.160.2.210:5060 -> 192.160.2.60:5060 Call-ID: becd0e00-75018675-b61d-5932e80a@10.232.50.89 Caller uri: sip:7814437285@192.160.2.210 Callee uri: sip:19123037947@192.160.2.60	From tag: 160250-00b97701-5e47-02c7-c4f0-73777b880ae3-18960193 Last response code: 200 Caller device: Cisco-CUCM10.5	Status: Finished

Link Quality
No Data Available

Voice Quality
No Data Available

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



Phase 3 – Configuring the Cisco Unified Communications Manager (CUCM)

The enterprise has a fully functional Cisco CUCM. Backup the existing configuration before proceeding. Configuring CUCM to operate with the Oracle E-SBC consists of the following steps:

- Generating a Certificate Signing Request (CSR) for CallManager
- Importing the Certificate Authority (CA) certificate
- Importing the CallManager certificate signed by a CA
- Configuring a SIP Trunk Security Profile
- Creating a SIP Profile
- Configuring a SIP Trunk
- Creating a Route Pattern
- Setting the cluster to Mixed Mode

Generating a Certificate Signing Request (CSR) for CallManager

Log in to the Cisco Unified OS Administration.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go

Username

Password

Login Reset

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

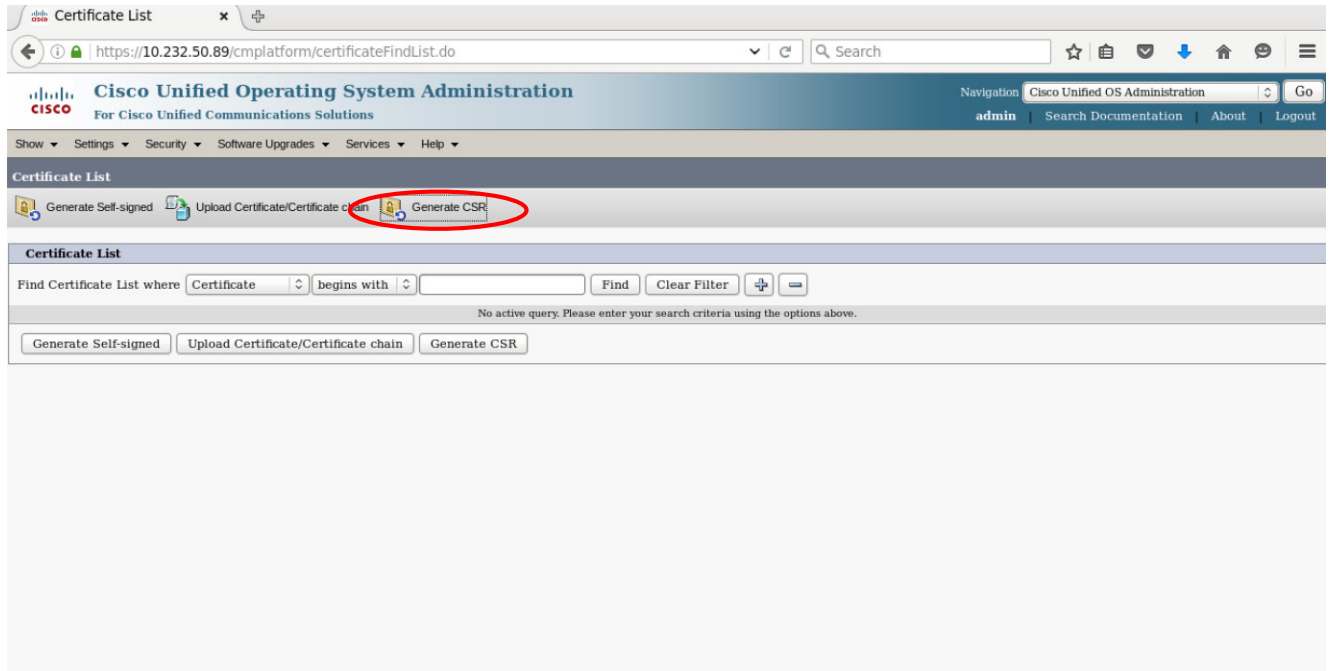
A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

early Highlight All Match Case 5 of 5 matches



Click on Generate CSR.




Choose "CallManager" as the Certificate Purpose. Select a distribution, and then enter CUCM's Fully Qualified Domain Name (FQDN) as the Common Name. Leave the Subject Alternate Names (SANs) Parent Domain blank. Select 2048 as the Key Length, and SHA256 as the Hash Algorithm. Then click on Generate.

https://10.232.50.89/cmplatform/certificateGenerateNewCsr.do

Generate Certificate Signing Request

 Generate  Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*

Distribution*


Common Name*

Subject Alternate Names (SANs)

Parent Domain

Key Length*

Hash Algorithm*

 *- indicates required item.

You will see a list of certificates. Click on the FQDN that has “CSR Only” listed as the type.

The screenshot shows the Cisco Unified Operating System Administration interface. The page title is "Certificate List" and the URL is "https://10.232.50.89/cmplatform/certificateFindList.do". The interface includes a navigation bar with "admin" and "Search Documentation" links. Below the navigation bar, there are several action buttons: "Generate Self-signed", "Upload Certificate/Certificate chain", "Generate CSR", and "Download CSR". A status bar indicates "26 records found". The main content area displays a table of certificates with the following columns: Certificate, Common Name, Type, Distribution, Issued By, Expiration, and Description. The first row in the table has "CUCM-Cisco.pe.oracle.com" circled in red in the Common Name column and "CSR Only" in the Type column.

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM-Cisco.pe.oracle.com	CSR Only	CUCM-Cisco.pe.oracle.com	--	--	
CallManager	CUCM-Cisco.pe.oracle.com	Self-signed	CUCM-Cisco.pe.oracle.com	CUCM-Cisco.pe.oracle.com	02/23/2020	Self-signed certificate generated by system
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	
CallManager-trust	Oracle_PE_Lab_CA	Self-signed	Oracle_PE_Lab_CA	Oracle_PE_Lab_CA	09/14/2020	Oracle Lab CA Certificate
CallManager-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/06/2023	Oracle Lab CA Certificate
CallManager-trust	CAPF-96f925ca	Self-signed	CAPF-96f925ca	CAPF-96f925ca	02/23/2020	Oracle Lab CA Certificate
CallManager-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	Oracle Lab CA

Click on Download CSR.

CSR Details - Mozilla Firefox

https://10.232.50.89/cmplatform/certificateEdit.do?csr=/usr/local/cm/.security/CallManager/

CSR Details for CUCM-Cisco.pe.oracle.com, CallManager

Delete Download CSR

Status

Status: Ready

Certificate Settings

File Name	CallManager.csr
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	

Certificate File Data

```
PKCS10 Request: [
Version: 0
Subject: SERIALNUMBER=95020c18aa28717e651c4973f9b6cabdcf34bfe2118ece345fa8aa21ce0e796d,
CN=CUCM-Cisco.pe.oracle.com, OU=Lab, O=Oracle, L=Boston, ST=MA, C=US
SubjectPKInfo: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100927678a0a5ec934c57df4c576c639b66f4ba3a4a32240297a4e13567acd88056c953a6f41cdf30
04be3e79fddb7dc8e23ce97d9226348409520f02d3999c5ffb1de4eb5e4fee1f092cdf72f6d3d735e04a9f54b3653962b9b
26ed09e23f2375902f3c2186260573bfd2f0d5b6f59f91afe80e5e7c072cf32d3c5a0be1ddc33d07c47ed85bae66060fe30
e9e65051c91fbf2d4c76d47c9c2426efe02b18514e9123ad076940237225d2647a2eef91738bc4ca91200a4c39177007
cce20d9f00338c374b626101fa58693c7b3d090171894a0656ea7d77bdf6e904ece25353430f4060d72358912127ddb8
6a1ee02c4812ea0c40e7491022a623487bfe39f55d610203010001
Attributes: [
Requested Extensions [
ExtKeyUsage [
1.3.6.1.5.5.7.3.1
```

Delete Download CSR

Close

Click on Save File and save the file to your PC or server.

The screenshot displays a web browser window with the title "CSR Details for CUCM-Cisco.pe.oracle.com, CallManager". At the top, there are two buttons: "Delete" (with a red X icon) and "Download CSR" (with a download icon). Below this is a "Status" section showing "Status: Ready" with an information icon. The "Certificate Settings" section lists: File Name: CallManager.csr, Certificate Purpose: CallManager, Certificate Type: ..., Certificate Group: ..., and Description (fr... The "Certificate File" section shows PKCS10 Request details: Version: 0, Subject: SERIAL CN=CUCM-Cis, SubjectPKInfo: ..., Key value: 3082010a02820...cdf3004be3e79fd9db7dc8e23ce97d9226348409520f02d3999c5ffb1de4eb5e4fee1f092cdf72f6d3d735e04a9f54b3653962b9b26ed09e23f2375902f3c2186260573bfd2f0d5b6f59f91afe80e5e7c072cf32d3c5a0be1ddc33d07c47ed85bae66060fe30e9e65051c91fbf2d4c76d47c9c2426efe02b18514e9123ad076940237225d2647a2eef91738bc4ca91200a4c39177007cce20d9f00338c374b626101fa58693c7b3d090171894a0656ea7d77bdf6e904ece25353430f4060d72358912127ddb86a1ee02c4812ea0c40e7491022a623487bfe39f55d610203010001. Attributes: [Requested Extensions [ExtKeyUsage [1.3.6.1.5.5.7.3.1. At the bottom of the main window are "Delete" and "Download CSR" buttons. A "Close" button is visible at the bottom left of the browser window. The modal dialog box "Opening CallManager.csr" is centered, showing "You have chosen to open: CallManager.csr which is: BIN file (1.2 KB) from: https://10.232.50.89" and "Would you like to save this file?". It has "Cancel" and "Save File" buttons, with "Save File" circled in red.

Send the CallManager.csr file to your Certificate Authority to be signed.

Importing the Certificate Authority (CA) Certificate

Import the Certificate Authority's (CA's) certificate in PEM format to the CallManager-trust store. Click on Upload Certificate/Certificate Chain.

The screenshot shows the Cisco Unified Operating System Administration interface. The page title is "Certificate List". The navigation bar includes "Cisco Unified OS Administration" and "admin". The main content area has a "Certificate List" header and a toolbar with buttons: "Generate Self-signed", "Upload Certificate/Certificate chain" (circled in red), "Generate CSR", and "Download CSR". Below the toolbar, a status bar shows "26 records found". A table titled "Certificate List (1 - 26 of 26)" displays the following data:

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM-Cisco.pe.oracle.com	CSR Only	CUCM-Cisco.pe.oracle.com	--	--	
CallManager	CUCM-Cisco.pe.oracle.com	Self-signed	CUCM-Cisco.pe.oracle.com	CUCM-Cisco.pe.oracle.com	02/23/2020	Self-signed certificate generated by system
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	
CallManager-trust	Oracle_PE_Lab_CA	Self-signed	Oracle_PE_Lab_CA	Oracle_PE_Lab_CA	09/14/2020	Oracle Lab CA Certificate
CallManager-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/06/2023	Oracle Lab CA Certificate
CallManager-trust	CAPF-96F925ca	Self-signed	CAPF-96F925ca	CAPF-96F925ca	02/23/2020	Oracle Lab CA Certificate
CallManager-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	Oracle Lab CA

For the Certificate Purpose, select CallManager-trust and give it a description. Click on Browse to find the CA certificate file on your local PC or server. Then click on Upload.

Upload Certificate/Certificate chain - Mozilla Firefox

https://10.232.50.89/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name) Oracle Lab CA Certificate

Upload File Browse... ca-cert.pem

Upload Close

i *- indicates required item.

You should see "Success: Certificate Uploaded".

The screenshot shows a Mozilla Firefox browser window titled "Upload Certificate/Certificate chain - Mozilla Firefox". The address bar displays the URL "https://10.232.50.89/cmplatform/certificateUpload.do". The page content includes a header "Upload Certificate/Certificate chain" with "Upload" and "Close" buttons. A "Status" section shows a message: "Success: Certificate Uploaded". Below this is a form titled "Upload Certificate/Certificate chain" with fields for "Certificate Purpose*" (set to "CallManager-trust"), "Description(friendly name)", and "Upload File" (with a "Browse..." button and "No file selected." text). At the bottom of the form are "Upload" and "Close" buttons. A note at the bottom left states: "i *- indicates required item."

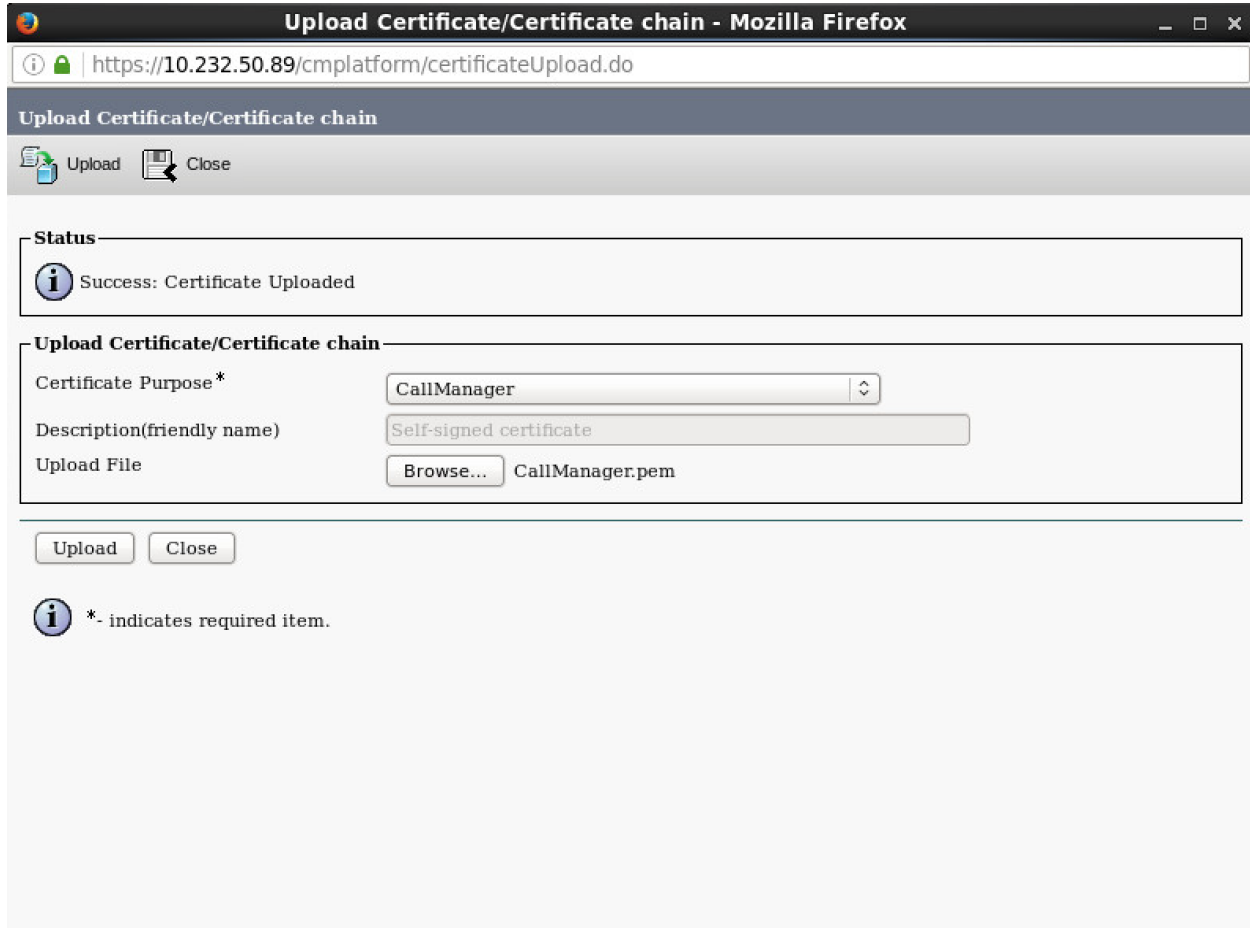
Importing the CallManager certificate signed by a CA

Import the CallManager certificate after it has been signed by the CA. Click on Upload Certificate/Certificate Chain.

The screenshot shows the Cisco Unified Operating System Administration interface. The browser address bar displays <https://10.232.50.89/cmplatform/certificateFindList.do>. The page title is "Certificate List". The navigation bar includes "Cisco Unified OS Administration" and "admin". The main content area has a "Certificate List" header and a toolbar with buttons: "Generate Self-signed", "Upload Certificate/Certificate chain" (circled in red), "Generate CSR", and "Download CSR". Below this is a "Status" box showing "26 records found". A search bar is present with "Find Certificate List where" and "begins with" dropdowns, and "Find" and "Clear Filter" buttons. The main table displays the following data:

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM-Cisco.pe.oracle.com	CSR Only	CUCM-Cisco.pe.oracle.com	--	--	
CallManager	CUCM-Cisco.pe.oracle.com	Self-signed	CUCM-Cisco.pe.oracle.com	CUCM-Cisco.pe.oracle.com	02/23/2020	Self-signed certificate generated by system
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	
CallManager-trust	Oracle_PE_Lab_CA	Self-signed	Oracle_PE_Lab_CA	Oracle_PE_Lab_CA	09/14/2020	Oracle Lab CA Certificate
CallManager-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/06/2023	Oracle Lab CA Certificate
CallManager-trust	CAPF-96f925ca	Self-signed	CAPF-96f925ca	CAPF-96f925ca	02/23/2020	Oracle Lab CA Certificate
CallManager-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	Oracle Lab CA

Select CallManager as the Certificate Purpose. Click Browse to find the signed certificate on your PC or server. Then click Upload.



You should see "Success: Certificate Uploaded".

Configuring a SIP Trunk Security Profile

Navigate to Cisco Unified CM Administration and login.

Cisco Unified CM Administration

For Cisco Unified Communications Solutions

Cisco Unified CM Administration

Username

Password

Login Reset

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Click on System.

Window Menu jed CM Co... x

https://10.232.50.89/ccmadmin/showHome.do

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
admin Search Documentation About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

WARNING: It has been 5 day(s) without a successful backup. Please verify backup configuration.

Cisco Unified CM Administration

System version: 10.5.2.10000-5

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz, disk 1: 80Gbytes, 8192Mbytes RAM, Partitions aligned

Last Successful Backup: 5 day(s) ago

User admin last logged in to this cluster on Wednesday, June 1, 2016 4:09:21 PM EDT, to node 10.232.50.89, from 10.232.50.86 using HTTPS

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

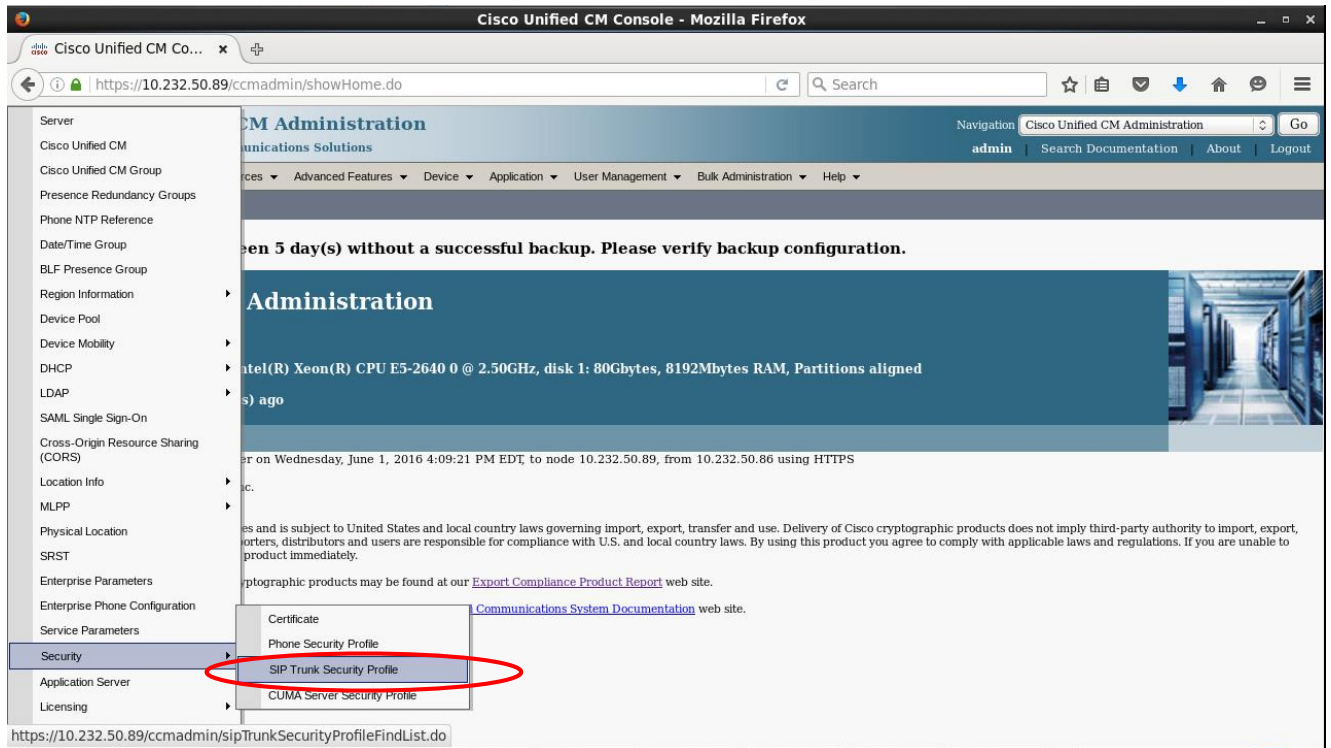
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Click on Security, then SIP Trunk Security Profile.



Click on Add New.

The screenshot shows a web browser window titled "Find and List SIP Trunk Security Profiles - Mozilla Firefox". The address bar shows the URL "https://10.232.50.89/ccmadmin/sipTrunkSecurityProfileFindList.do". The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". A navigation menu is visible with options like "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is titled "Find and List SIP Trunk Security Profiles" and contains an "Add New" button with a plus icon. Below this is a search section for "SIP Trunk Security Profile" with dropdown menus for "Name" and "begins with", and buttons for "Find" and "Clear Filter". A message below the search section reads "No active query. Please enter your search criteria using the options above." At the bottom of the search section, the "Add New" button is circled in red.

Give the trunk a name. "SIP Trunk Security Profile – TLS Test Trunk" is used in this example. Select Encrypted as the Device Security Mode, and TLS as both the Incoming and Outgoing Transport Type. Enter the SBC's FQDN from the SBC's certificate's Common Name in the X.509 Subject Name field. "trunking-sbc.pe.oracle.com" is used in this example. This is the common-name in the SBC's certificate-record. Make sure the Incoming Port is set to 5061.

The screenshot displays the Cisco Unified CM Administration web interface for configuring a SIP Trunk Security Profile. The browser window title is "SIP Trunk Security Profile Configuration - Mozilla Firefox". The URL is "https://10.232.50.89/ccmadmin/sipTrunkSecurityProfileEdit.do?key=9c7efc62-10e7-85fd-516b-b7". The page header shows "Cisco Unified CM Administration" with a navigation menu and user information (admin). The main content area is titled "SIP Trunk Security Profile Configuration" and includes a "Status: Ready" indicator. Below this, the "SIP Trunk Security Profile Information" section contains the following configuration fields:

- Name*: SIP Trunk Security Profile - TLS Test Trunk
- Description: (empty)
- Device Security Mode: Encrypted
- Incoming Transport Type*: TLS
- Outgoing Transport Type: TLS
- Enable Digest Authentication:
- Nonce Validity Time (mins)*: 600
- X.509 Subject Name: trunking-sbc.pe.oracle.com
- Incoming Port*: 5061
- Enable Application level authorization:
- Accept presence subscription:
- Accept out-of-dialog refer**:
- Accept unsolicited notification:
- Accept replaces header:

The remaining checkboxes should be selected as shown below. Then click Save.

The screenshot displays the 'SIP Trunk Security Profile Configuration' page in the Cisco Unified CM Administration interface. The page title is 'SIP Trunk Security Profile Configuration - Mozilla Firefox'. The URL is 'https://10.232.50.89/ccmadmin/sipTrunkSecurityProfileEdit.do?key=9c7efc62-10e7-85fd-516b-b7'. The page header includes the Cisco logo and 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. The navigation menu shows 'admin' and links for 'Search Documentation', 'About', and 'Logout'. The main content area is titled 'SIP Trunk Security Profile Configuration' and includes a 'Related Links' section with 'Back To Find/List'. The configuration options are as follows:

- Outgoing Transport Type: TLS
- Enable Digest Authentication:
- Nonce Validity Time (mins)*: 600
- X.509 Subject Name: trunking-sbc.pe.oracle.com
- Incoming Port*: 5061
- Enable Application level authorization:
- Accept presence subscription:
- Accept out-of-dialog refer**:
- Accept unsolicited notification:
- Accept replaces header:
- Transmit security status:
- Allow charging header:
- SIP V.150 Outbound SDP Offer Filtering*: Use Default Filter

At the bottom of the configuration area, there are buttons for 'Save', 'Delete', 'Copy', 'Reset', 'Apply Config', and 'Add New'. Below the configuration area, there are two informational messages:

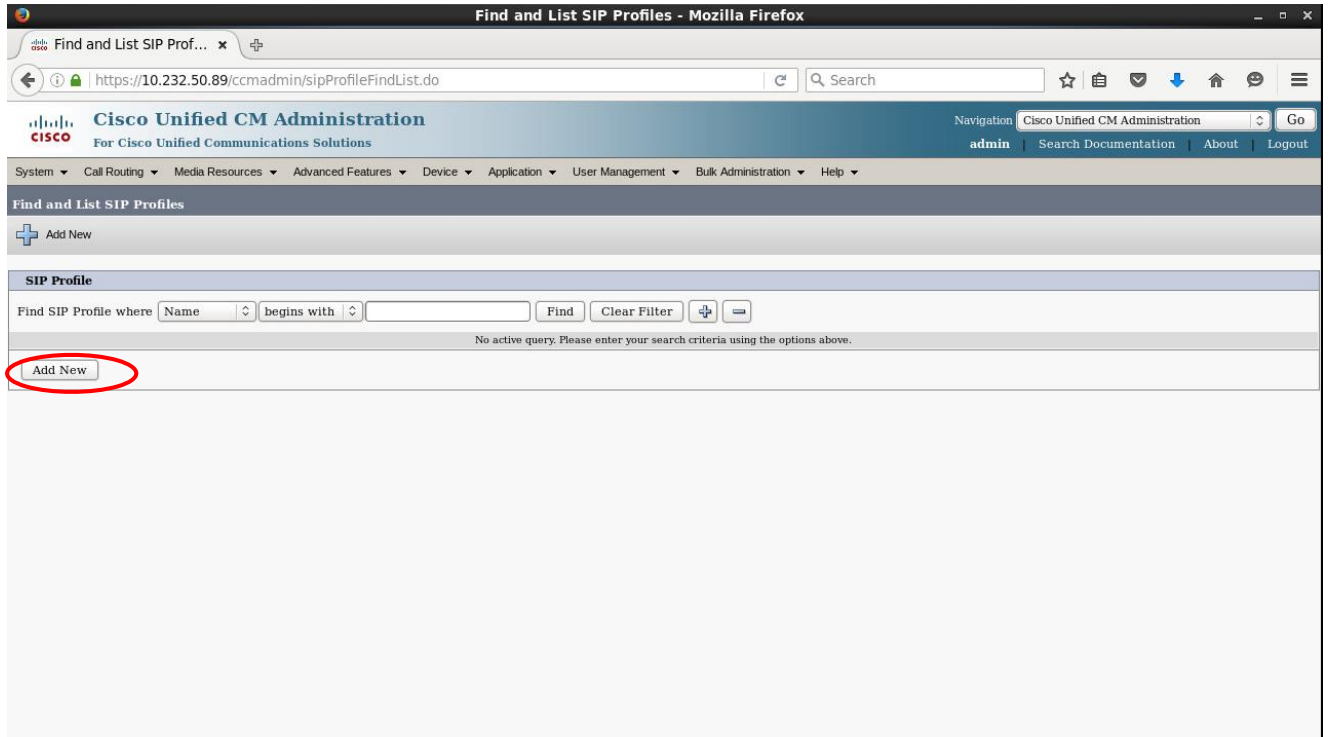
- i** *: indicates required item.
- i** **: If this profile is associated with an EMCC SIP trunk, Accept Out-of-Dialog REFER is enabled regardless of the setting on this page

Creating a SIP Profile

Click on Device, then Device Settings, then SIP Profile.

The screenshot shows the Cisco Unified CM Administration web interface in a Mozilla Firefox browser. The address bar displays the URL `https://10.232.50.89/ccmadmin/showHome.do`. The page header includes the Cisco logo and the title "Cisco Unified CM Administration For Cisco Unified Communications Solutions". A navigation bar at the top contains the following menu items: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The "Device" menu is expanded, showing a list of options: CTI Route Point, Gatekeeper, Gateway, Phone, Trunk, Remote Destination, and Device Settings. The "Device Settings" option is further expanded into a sub-menu, where "SIP Profile" is highlighted with a red circle. Other items in the sub-menu include Device Defaults, Firmware Load Information, Default Device Profile, Device Profile, Phone Button Template, Softkey Template, Phone Services, Common Device Configuration, Common Phone Profile, Remote Destination Profile, Feature Control Policy, Recording Profile, SIP Normalization Script, SDP Transparency Profile, Network Access Profile, Wireless LAN Profile, Wireless LAN Profile Group, and Wi-Fi Hotspot Profile. The main content area of the page displays a warning message: "WARNING: It has been 5 day(s) without backup." Below the warning, the page title "Cisco Unified CM Administration" is visible, along with system information: "System version: 10.5.2.10000-5", "VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz, 4GB 4.00GB/s", and "Last Successful Backup: 5 day(s) ago". At the bottom of the page, there is a small text box containing the code `javascript:void(0)`.

Click on Add New.



Use "Standard SIP Profile – Early Offer" as the Name.

SIP Profile Configuration - Mozilla Firefox

Navigation: Cisco Unified CM Administration | admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SIP Profile Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

Status

- Status: Ready
- All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name* | Standard SIP Profile - Early Offer

Description |

Default MTP Telephony Event Payload Type* | 101

Early Offer for G.Clear Calls* | Disabled

User-Agent and Server header information* | Send Unified CM Version Information as User-Agent

Version in User Agent and Server Header* | Major And Minor

Dial String Interpretation* | Phone number consists of characters 0-9, *, #, an

Confidential Access Level Headers* | Disabled

Redirect by Application

Disable Early Media on 180

Outgoing T.38 INVITE include audio mline

Use Fully Qualified Domain Name in SIP Requests

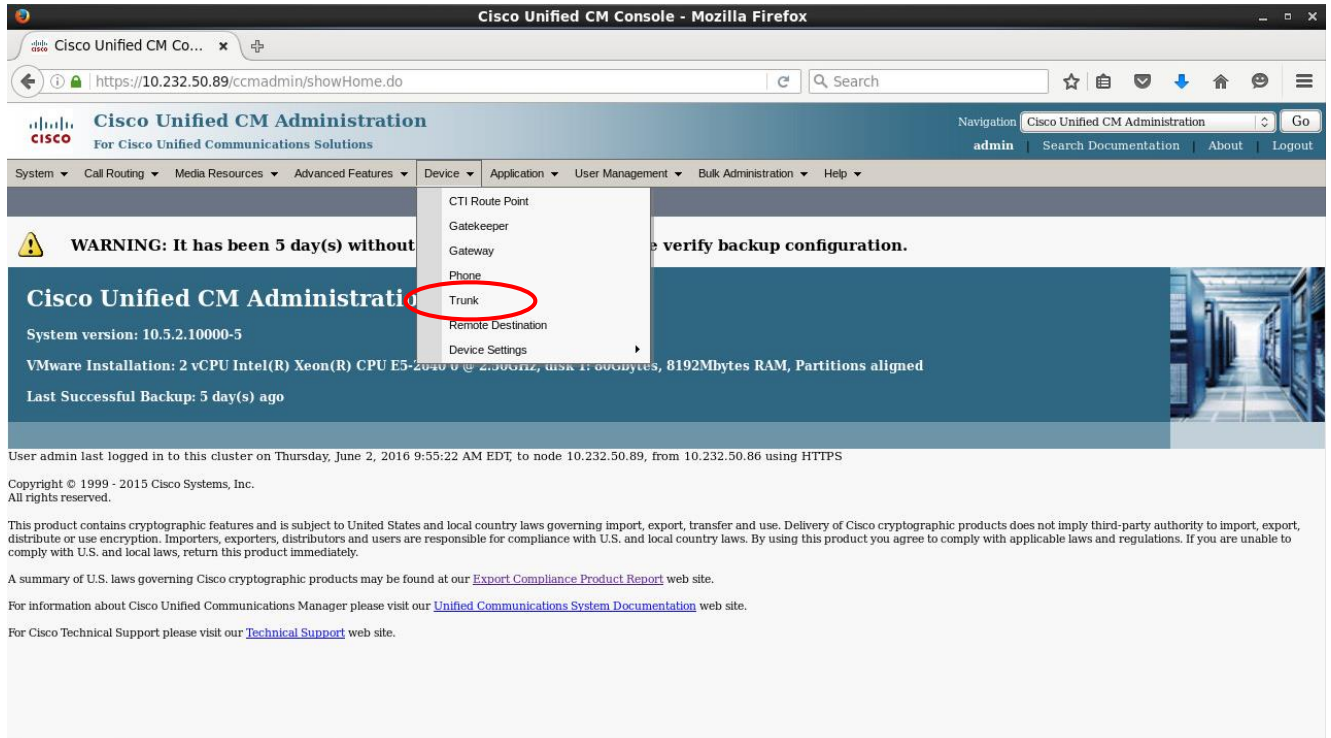
Assured Services SIP conformance

Scroll down to the Trunk Specific Configuration. Select “Mandatory (insert MTP if needed)” next to the Early Offer support for voice and video calls. Then click on Save.

The screenshot shows the Cisco Unified CM Administration interface for SIP Profile Configuration. The page title is "SIP Profile Configuration - Mozilla Firefox". The URL is "https://10.232.50.89/ccmadmin/sipProfileEdit.do?key=5aa37799-d7b8-53a0-2826-f3d5e5513506". The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is titled "SIP Profile Configuration" and includes a "Related Links" section with "Back To Find/List". Below this are action buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. The "Trunk Specific Configuration" section contains several dropdown menus and checkboxes. The "Early Offer support for voice and video calls*" dropdown menu is set to "Mandatory (insert MTP if needed)", which is highlighted by a red arrow. Other dropdown menus include "Reroute Incoming Request to new Trunk based on*" (Never), "RSVP Over SIP*" (Local RSVP), "Resource Priority Namespace List" (< None >), "SIP Re1XX Options*" (Disabled), "Video Call Traffic Class*" (Mixed), "Calling Line Identification Presentation*" (Default), and "Session Refresh Method*" (Invite). Checkboxes include "Fall back to local RSVP" (checked), "Enable ANAT", "Deliver Conference Bridge Identifier", "Allow Passthrough of Configured Line Device Caller Information", "Reject Anonymous Incoming Calls", "Reject Anonymous Outgoing Calls", and "Send ILS Learned Destination Route String". The "SIP OPTIONS Ping" section has a checkbox for "Enable OPTIONS Ping to monitor destination status for Trunks with Service Type 'None (Default)'" which is unchecked.

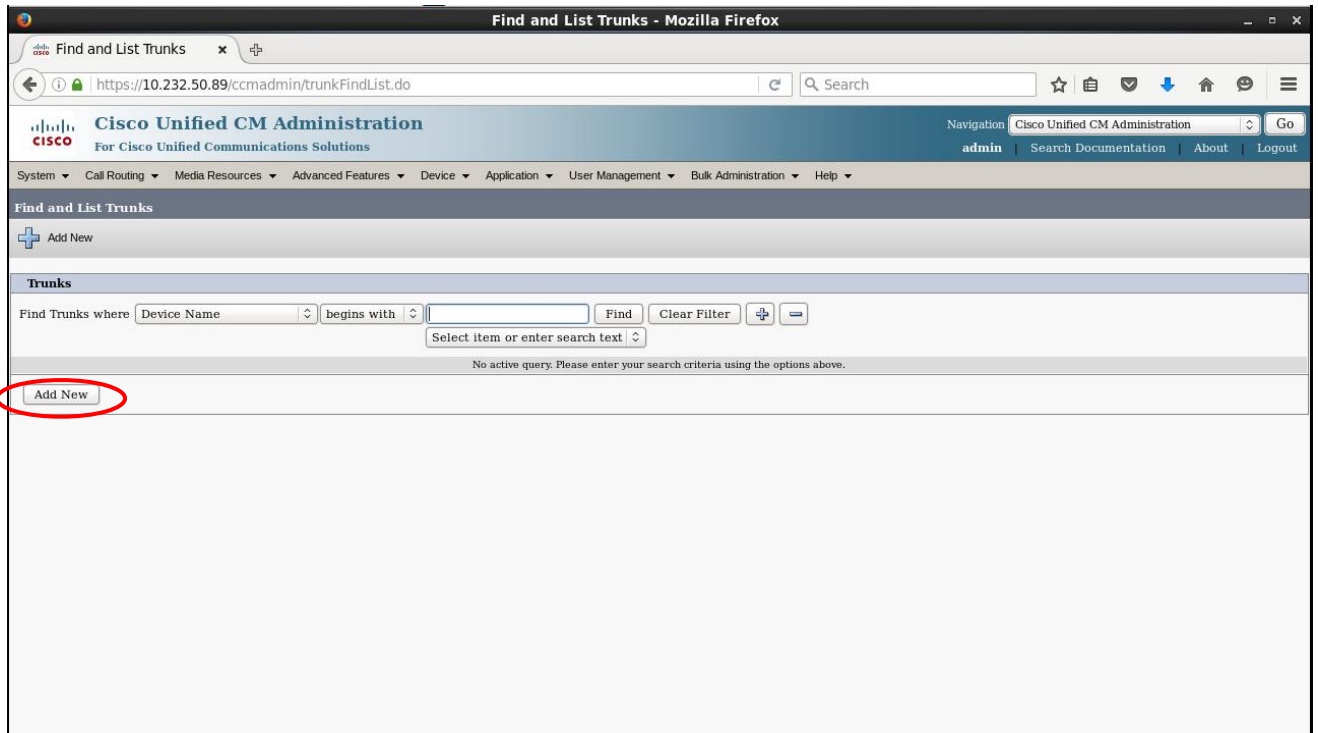
Configuring a SIP Trunk

Click on Device, then Trunk.



The screenshot shows the Cisco Unified CM Administration web interface in a Mozilla Firefox browser. The address bar displays the URL <https://10.232.50.89/ccmadmin/showHome.do>. The page title is "Cisco Unified CM Administration" and the navigation menu includes "admin", "Search Documentation", "About", and "Logout". The main navigation bar contains "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The "Device" menu is open, showing a list of options: "CTI Route Point", "Gatekeeper", "Gateway", "Phone", "Trunk", "Remote Destination", and "Device Settings". The "Trunk" option is circled in red. The main content area displays a warning message: "WARNING: It has been 5 day(s) without backup configuration." Below the warning, the page title "Cisco Unified CM Administration" is partially visible, along with system information: "System version: 10.5.2.10000-5", "VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5-2640 v @ 2.50GHz, ussr 1: 600bytes, 8192Mbytes RAM, Partitions aligned", and "Last Successful Backup: 5 day(s) ago". At the bottom of the page, there is a footer with copyright information and links to "Export Compliance Product Report", "Unified Communications System Documentation", and "Technical Support" web sites.

Click on Add New.



Give the trunk a name. SIP_TLS_Test_Trunk was used in this example. Set the other values shown below as appropriate for your CUCM installation.

The screenshot shows the Cisco Unified CM Administration web interface in Mozilla Firefox. The page title is "Trunk Configuration - Mozilla Firefox". The browser address bar shows the URL: <https://10.232.50.89/ccmadmin/trunkEdit.do?key=9378e7e1-8e92-6025-c32f-8e91994bc09e>. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is titled "Trunk Configuration" and includes a "Related Links" section with "Back To Find/List" and "Go". Below the title bar are icons for "Save", "Delete", "Reset", and "Add New". The configuration form is as follows:

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name *	<input type="text" value="SIP_TLS_Test_Trunk"/>
Description	<input type="text"/>
Device Pool*	<input type="text" value="Default"/>
Common Device Configuration	<input type="text" value="< None >"/>
Call Classification*	<input type="text" value="Use System Default"/>
Media Resource Group List	<input type="text" value="< None >"/>
Location*	<input type="text" value="Hub_None"/>
AAR Group	<input type="text" value="< None >"/>
Tunneled Protocol*	<input type="text" value="None"/>
QSIG Variant*	<input type="text" value="No Changes"/>
ASN.1 ROSE OID Encoding*	<input type="text" value="No Changes"/>
Packet Capture Mode*	<input type="text" value="None"/>
Packet Capture Duration	<input type="text" value="0"/>
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	

Scroll down to SIP Information. Enter the SBC's "cisco-core" sip-interface IP address and port 5061. Select the previously created SIP Trunk Security Profile. Select the previously created SIP Profile. Then click Save.

The screenshot shows the Cisco Unified CM Administration interface for Trunk Configuration. The page is titled "Trunk Configuration - Mozilla Firefox" and the URL is "https://10.232.50.89/ccmadmin/trunkEdit.do?key=9378e7e1-8e92-6025-c32f-8e91994bc09e". The navigation bar includes "Cisco Unified CM Administration" and "admin". The main content area is titled "Trunk Configuration" and has a "Related Links" section with "Back To Find/List".

The "SIP Information" section is expanded, showing a table with the following data:

Destination	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason
1*	10.232.50.100		5061	N/A	N/A

Below the table, the following configuration options are visible:

- MTP Preferred Originating Codec*: 711ulaw
- BLF Presence Group*: Standard Presence group
- SIP Trunk Security Profile*: SIP Trunk Security Profile - TLS Test Trunk
- Rerouting Calling Search Space: < None >
- Out-Of-Dialog Refer Calling Search Space: < None >
- SUBSCRIBE Calling Search Space: < None >
- SIP Profile*: Standard SIP Profile - Early Offer
- DTMF Signaling Method*: No Preference

The "Normalization Script" section is also visible, with "Normalization Script" set to "< None >" and "Enable Trace" unchecked. A "View Details" link is present next to the SIP Profile selection.

After saving, click on Reset, then click on Reset again in the pop up window.

The screenshot displays the Cisco Unified CM Administration interface in a Mozilla Firefox browser. The main window is titled "Trunk Configuration" and shows a "Trunk Configuration" page with a "Reset" button circled in red. A "Device Reset" pop-up window is open, also titled "Device Reset - Mozilla Firefox". The pop-up window contains the following information:

- Device Reset** (Section Header)
- Status** (Section Header)
- Status:** Ready
- Reset Information** (Section Header)
- Selected Device:** SIP_TLS_Test_Trunk (SIP Trunk)
- Note:** Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.
- Buttons:** Reset, Restart, Close (The "Reset" button is circled in red).

Creating a Route Pattern

Click on Call Routing.

Cisco Unified CM Console - Mozilla Firefox

https://10.232.50.89/ccmadmin/showHome.do

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin Search Documentation About Logout

System **Call Routing** Media Resources Advanced Features Device Application User Management Bulk Administration Help

WARNING: It has been 5 day(s) without a successful backup. Please verify backup configuration.

Cisco Unified CM Administration

System version: 10.5.2.10000-5

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz, disk 1: 80Gbytes, 8192Mbytes RAM, Partitions aligned

Last Successful Backup: 5 day(s) ago

User admin last logged in to this cluster on Thursday, June 2, 2016 9:55:22 AM EDT, to node 10.232.50.89, from 10.232.50.86 using HTTPS

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Click on Route/Hunt, then Route Pattern.

Cisco Unified CM Console - Mozilla Firefox

Navigation: Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

Advanced Features Device Application User Management Bulk Administration Help

Backup. Please verify backup configuration.

disk 1: 80Gbytes, 8192Mbytes RAM, Partitions aligned

May, June 2, 2016 9:55:22 AM EDT, to node 10.232.50.89, from 10.232.50.86 using HTTPS

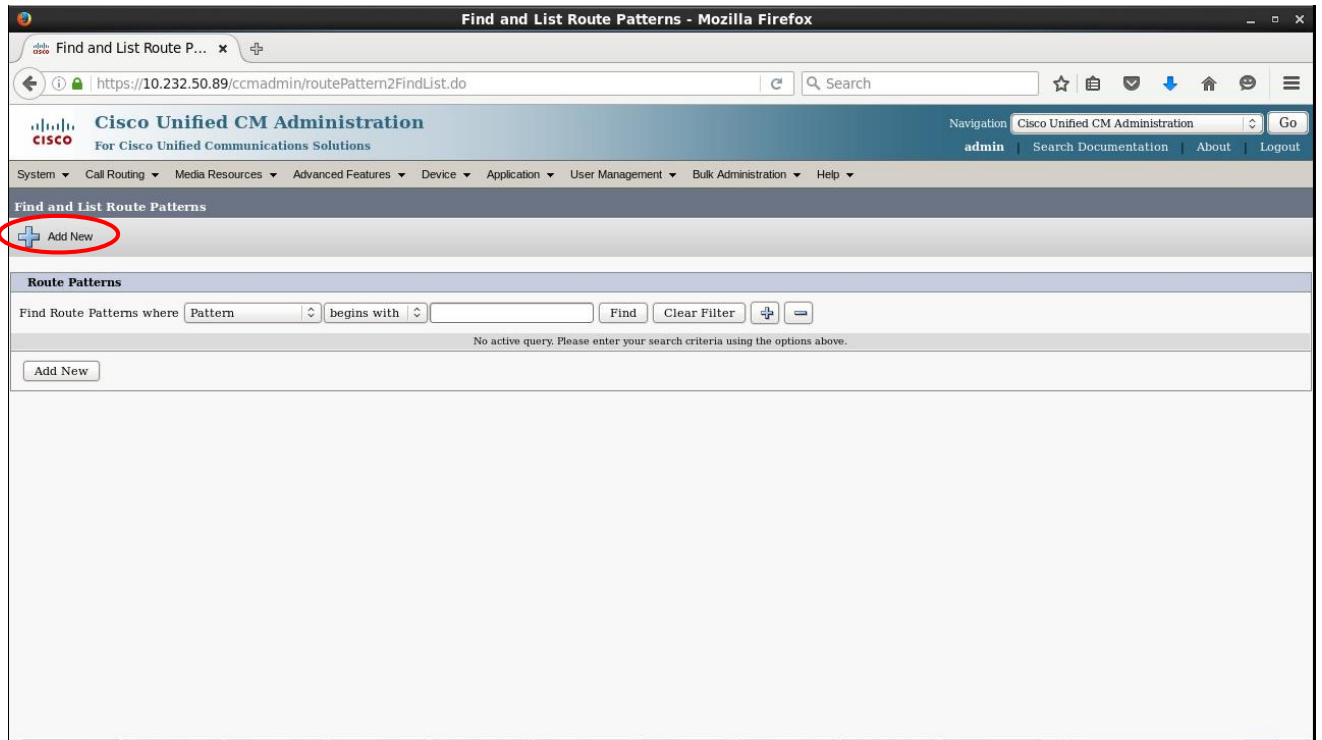
subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use. Users and administrators are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with applicable laws and regulations, you should not use this product. For more information on product restrictions, visit our [Export Compliance Product Report](#) web site.

For more information on product restrictions, visit our [Unified Communications System Documentation](#) web site.

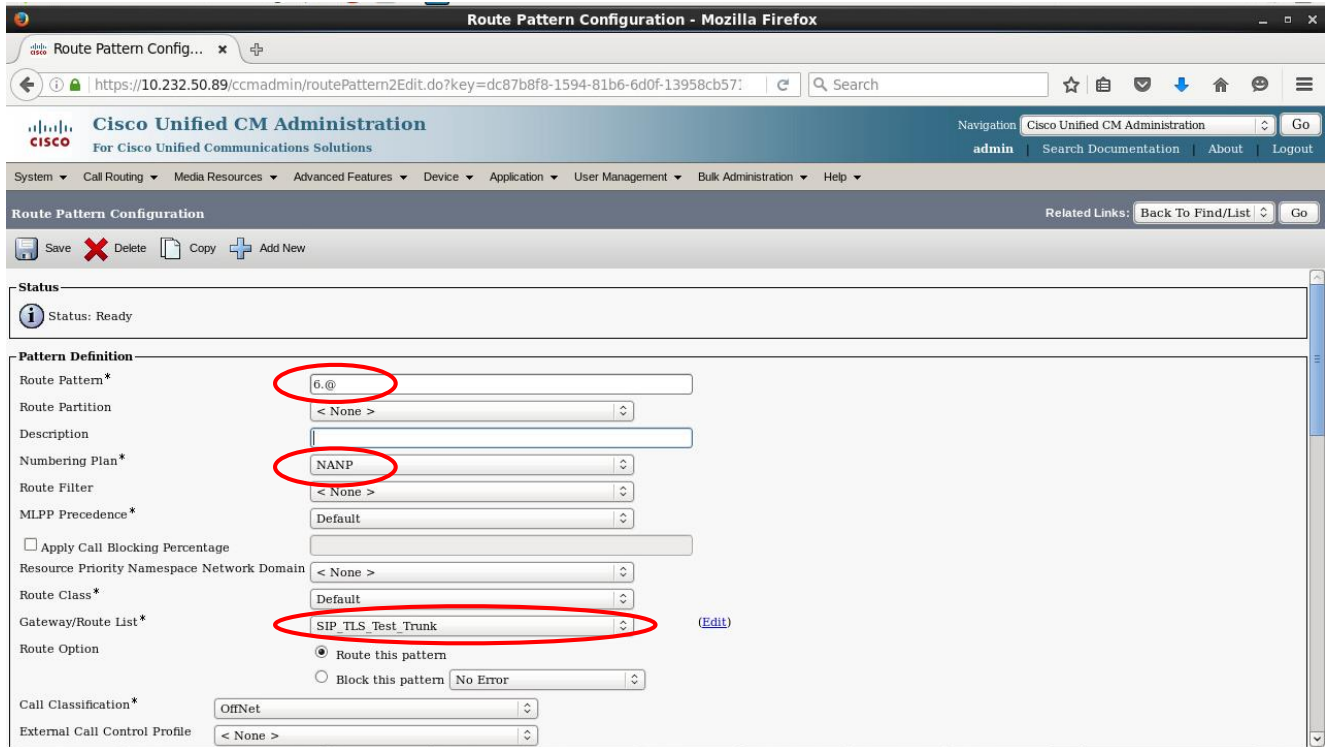
For more information on product restrictions, visit our [Support](#) web site.

https://10.232.50.89/ccmadmin/routePattern2FindList.do

Click on Add New.



Enter an appropriate Route Pattern for your network. In this example, 6.@ was used which basically means that any number dialed beginning with 6 will route out the trunk. Select the Numbering Plan that is relevant to your network (NANP, or North American Numbering Plan, was used here). Select the previously configured trunk from the Gateway/Route List.



Scroll down to the Called Party Transformations. Select "PreDot" next to Discard Digits. This will discard the "6" in our example configuration. Then click on Save.

The screenshot shows the Cisco Unified CM Administration interface for Route Pattern Configuration. The page title is "Route Pattern Configuration - Mozilla Firefox". The browser address bar shows the URL: <https://10.232.50.89/ccmadmin/routePattern2Edit.do?key=dc87b8f8-1594-81b6-6d0f-13958cb571>. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes "admin", "Search Documentation", "About", and "Logout". The main content area is titled "Route Pattern Configuration" and includes a "Related Links" section with "Back To Find/List" and "Go".

The configuration form includes the following sections:

- Save, Delete, Copy, Add New** (Action buttons)
- Connected Line ID Presentation*** (Dropdown menu: Default)
- Connected Name Presentation*** (Dropdown menu: Default)
- Called Party Transformations**
 - Discard Digits** (Dropdown menu: PreDot - highlighted with a red circle)
 - Called Party Transform Mask** (Text input field)
 - Prefix Digits (Outgoing Calls)** (Text input field)
 - Called Party Number Type*** (Dropdown menu: Cisco CallManager)
 - Called Party Numbering Plan*** (Dropdown menu: Cisco CallManager)
- ISDN Network-Specific Facilities Information Element**
 - Network Service Protocol** (Dropdown menu: -- Not Selected --)
 - Carrier Identification Code** (Text input field)
 - Network Service** (Dropdown menu: -- Not Selected --)
 - Service Parameter Name** (Text input field: < Not Exist >)
 - Service Parameter Value** (Text input field)

At the bottom, there are "Save", "Delete", "Copy", and "Add New" buttons, and a note: "i * indicates required item."

Click on OK in the pop up window.

The screenshot shows the Cisco Unified CM Administration interface in a Mozilla Firefox browser window. The page title is "Route Pattern Configuration". The browser address bar shows the URL: <https://10.232.50.89/ccmadmin/routePattern2Edit.do?key=dc87b8f8-1594-81b6-6d0f-13958cb571>. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes "admin", "Search Documentation", "About", and "Logout". The main content area is titled "Route Pattern Configuration" and contains several sections: "Connected Line ID Presentation*" (Default), "Connected Name Presentation*" (Default), "Called Party Transformations" (Discard Digits: PreDot, Called Party Transform Mask, Prefix Digits (Outgoing Calls), Called Party Number Type*: Cisco CallManager, Called Party Numbering Plan*: Cisco CallManager), and "ISDN Network-Specific Facilities Information Element" (Network Service Protocol: -- Not Selected --, Carrier Identification Code, Network Service: -- Not Selected --, Service Parameter Name: < Not Exist >, Service Parameter Value). At the bottom, there are buttons for "Save", "Delete", "Copy", and "Add New". A modal dialog box is overlaid on the page with the following text: "The Authorization Code will not be activated. Press OK if you want to proceed and activate it at a later time. Press Cancel and check the Force Authorization Code checkbox if you want to activate it now." The dialog box has "Cancel" and "OK" buttons.

Click OK again in the next pop up box.

The screenshot shows the Cisco Unified CM Administration interface in a Mozilla Firefox browser. The page title is "Route Pattern Configuration". The browser address bar shows the URL: <https://10.232.50.89/ccmadmin/routePattern2Edit.do?key=dc87b8f8-1594-81b6-6d0f-13958cb571>. The page header includes the Cisco logo and "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The main content area is titled "Route Pattern Configuration" and includes a "Related Links" section with "Back To Find/List". The configuration form has several sections: "Connected Line ID Presentation*" (Default), "Connected Name Presentation*" (Default), "Called Party Transformations" (Discard Digits: PreDot, Called Party Transform Mask, Prefix Digits (Outgoing Calls), Called Party Number Type*: Cisco CallManager, Called Party Numbering Plan*: Cisco CallManager), and "ISDN Network-Specific Facilities Information Element" (Network Service Protocol: -- Not Selected --, Carrier Identification Code, Network Service: -- Not Selected --, Service Parameter Name: < Not Exist >, Service Parameter Value). At the bottom, there are buttons for "Save", "Delete", "Copy", and "Add New". A warning dialog box is overlaid on the form, containing the text: "Any update to this Route Pattern automatically resets the associated gateway or Route List" and a checkbox labeled "Prevent this page from creating additional dialogs". An "OK" button is at the bottom right of the dialog. A legend at the bottom left indicates that an asterisk (*) indicates a required item.

Setting the cluster to Mixed Mode

Care should be followed during this procedure. Follow all Cisco documentation, and perform it during a maintenance window.

Secure Shell (SSH) to CUCM using a program such as PuTTY. Login as an administrator (admin is the username in our example).

Issue the following command:

```
utils ctl set-cluster mixed-mode
```

Then issue the following command:

```
utils system restart
```

Then enter "yes" without the quotes. CUCM will reboot.

After the system reboots, login to CUCM's web interface and click on System.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

WARNING: It has been 5 day(s) without a successful backup. Please verify backup configuration.

Cisco Unified CM Administration
System version: 10.5.2.10000-5
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz, disk 1: 80Gbytes, 8192Mbytes RAM, Partitions aligned
Last Successful Backup: 5 day(s) ago

User admin last logged in to this cluster on Thursday, June 2, 2016 9:55:22 AM EDT, to node 10.232.50.89, from 10.232.50.86 using HTTPS

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

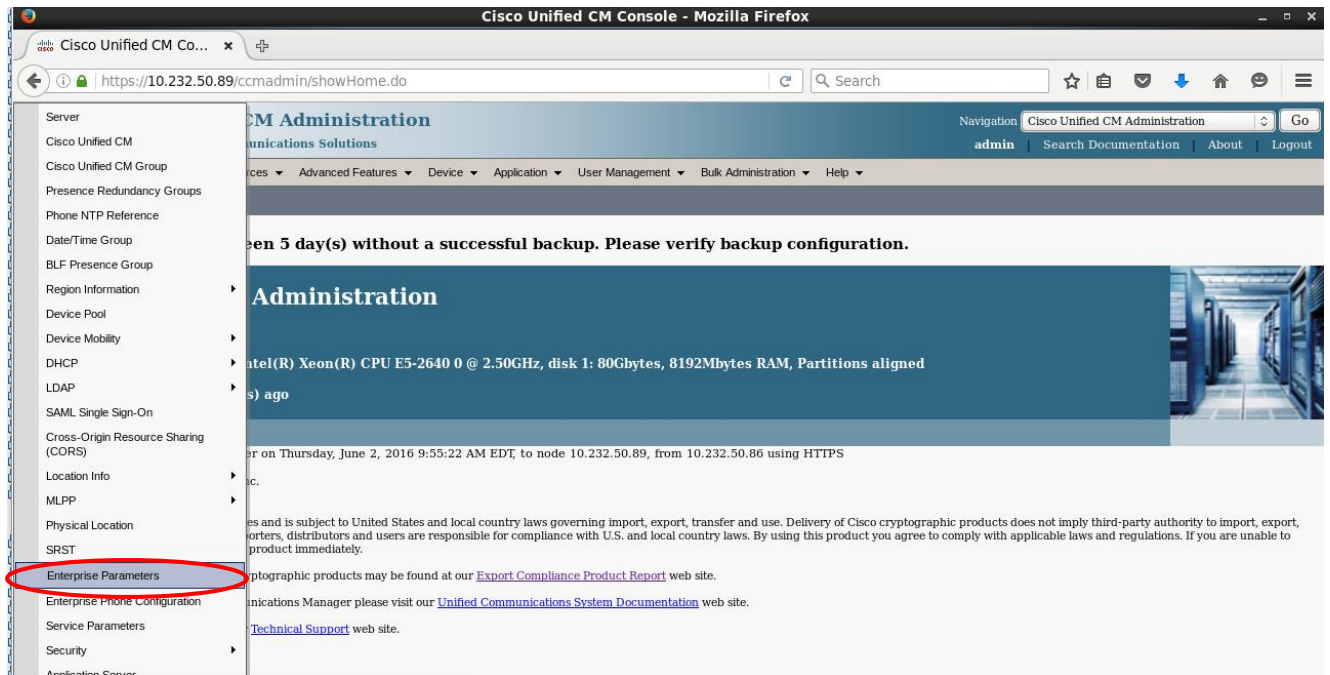
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Select Enterprise Parameters.



Scroll down to Security Parameters and verify the Cluster Security Mode is "1", indicating Mixed Mode.

The screenshot shows the 'Enterprise Parameters Configuration' page in the Cisco Unified CM Administration interface. The 'Cluster Security Mode' is set to '1', which is circled in red. Other parameters include 'Insecure Security Mode' (Insecure), 'CAPF Phone Port' (3804), 'CAPF Operation Expires in (days)' (10), 'Enable Caching' (True), 'TLS Ciphers' (All supported AES-256, AES-128 ciphers), 'SRTP Ciphers' (All supported AES-256, AES-128 ciphers), 'Certificate Validity Check' (Disabled), 'Validity Check Frequency (hours)' (24), 'Prepare Cluster for Rollback to pre 8.0' (False), 'URL Authentication' (http://CUCM-Cisco.pe.oracle.com:8080/ccmcp/autentic), 'URL Directories' (http://CUCM-Cisco.pe.oracle.com:8080/ccmcp/xmldirec), and 'URL Idle'.

Parameter	Value	Default
Cluster Security Mode *	1	
Insecure Security Mode *	Insecure	Insecure
CAPF Phone Port *	3804	3804
CAPF Operation Expires in (days) *	10	10
Enable Caching *	True	True
TLS Ciphers *	All supported AES-256, AES-128 ciphers	All supported AES-256, AES-128 ciphers
SRTP Ciphers *	All supported AES-256, AES-128 ciphers	All supported AES-256, AES-128 ciphers
Certificate Validity Check *	Disabled	Disabled
Validity Check Frequency (hours) *	24	24
Prepare Cluster for Rollback to pre 8.0 *	False	False
URL Authentication	http://CUCM-Cisco.pe.oracle.com:8080/ccmcp/autentic	
URL Directories	http://CUCM-Cisco.pe.oracle.com:8080/ccmcp/xmldirec	
URL Idle		

The configuration of CUCM is now complete.

Test Plans & Results

Test Plan

The test plan consisted of the following test cases.

Test Case	Result	Notes
Basic Call - Oubound	Pass	
Basic Call - Inbound	Pass	
Long Duration Call	Pass	20 minute call
Conference calling	Pass	Tested with 3 phones
Call Progress Tones	Pass	
Call Waiting	Pass	
Direct Outward Dialing	Pass	
Do Not Disturb (DND)	Pass	
Dual Tone Multi-Frequency signaling (DTMF) pass-through	Pass	Verified RFC 2833 RTP Event Packets were passed by the SBC.
Call Hold	Pass	
Consultation on Hold	Pass	
Call Transfer - supervised	Pass	
Call Transfer - blind	Pass	

Troubleshooting Tools

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

Wireshark

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

On the Oracle E-SBC

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

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

At the console:


```
oraclesbcl# reset sipd
oraclesbcl# notify sipd debug
oraclesbcl#
enabled SIP Debugging
oraclesbcl# 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 oraclesbclFTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

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

Through the Web GUI

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

Oracle Enterprise Operations Monitor (EOM)

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

Appendix A

Accessing the ACLI

Access to the ACLI is provided by:

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

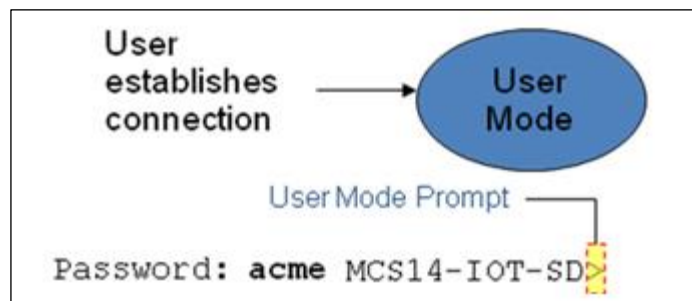
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

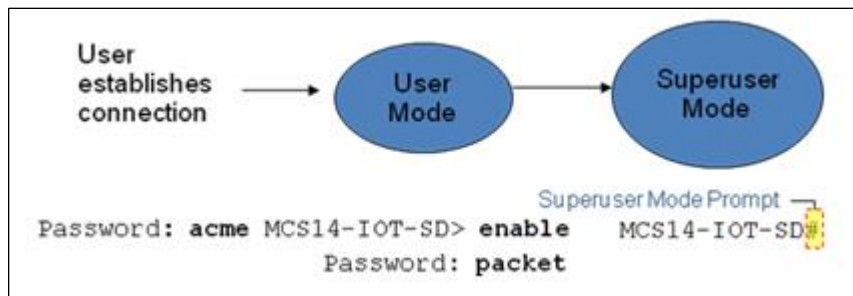
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

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

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



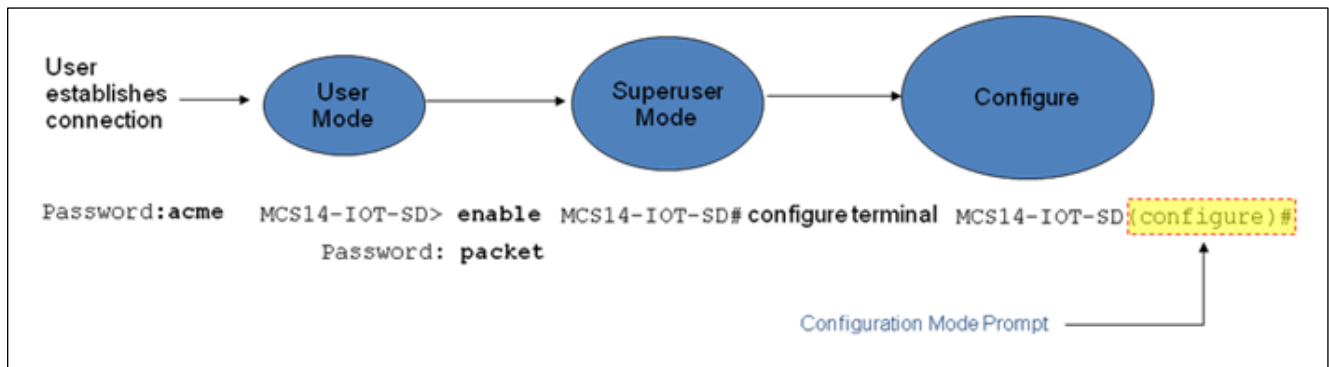
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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

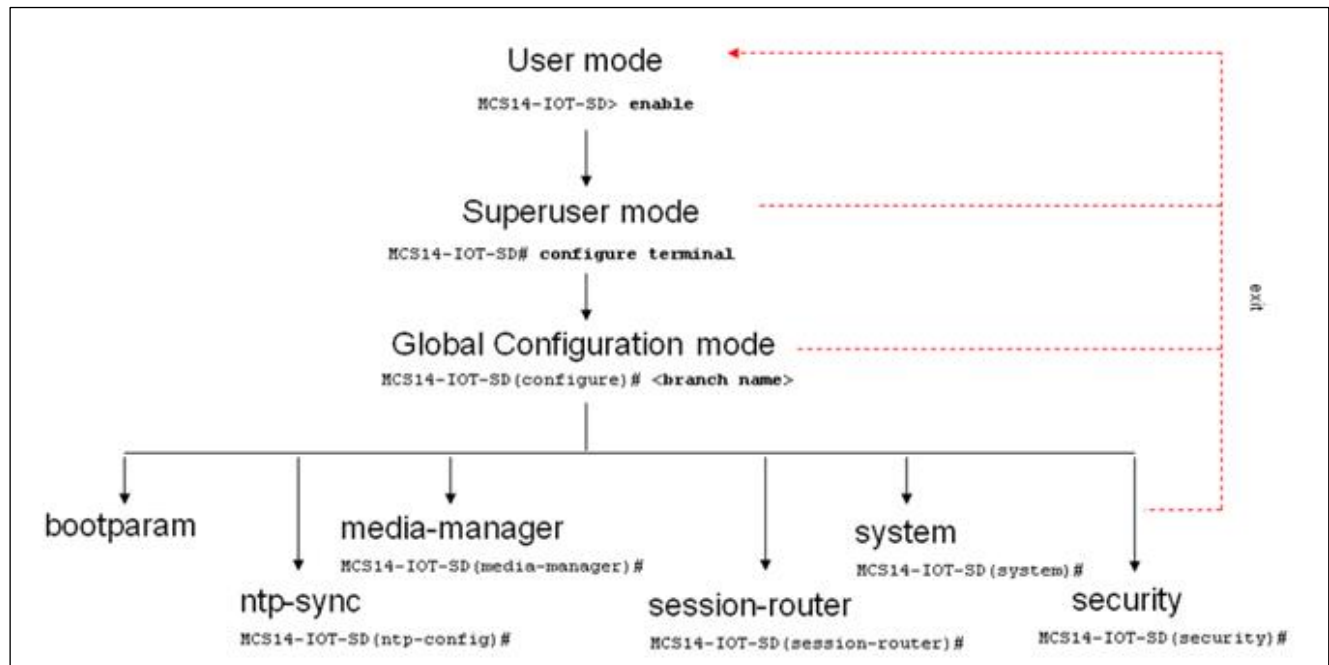
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the `configure terminal` command in the Superuser mode.

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



In the configuration mode, there are six configuration branches:

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



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

The `bootparam` branch provides access to SBC boot parameters.

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

The security branch provides access to security configuration.

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

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, ivf-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.

```
oraclesbcl # 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'.
oraclesbcl #
```

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.

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

ORACLE

CONNECT WITH US

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

Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615