ORACLE
COMMUNICATIONS

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

ORACLE

Disclaimer

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

Table of Contents

Intended Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Communications Enterprise-SBC, Oracle Enterprise Operations Monitor, and 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

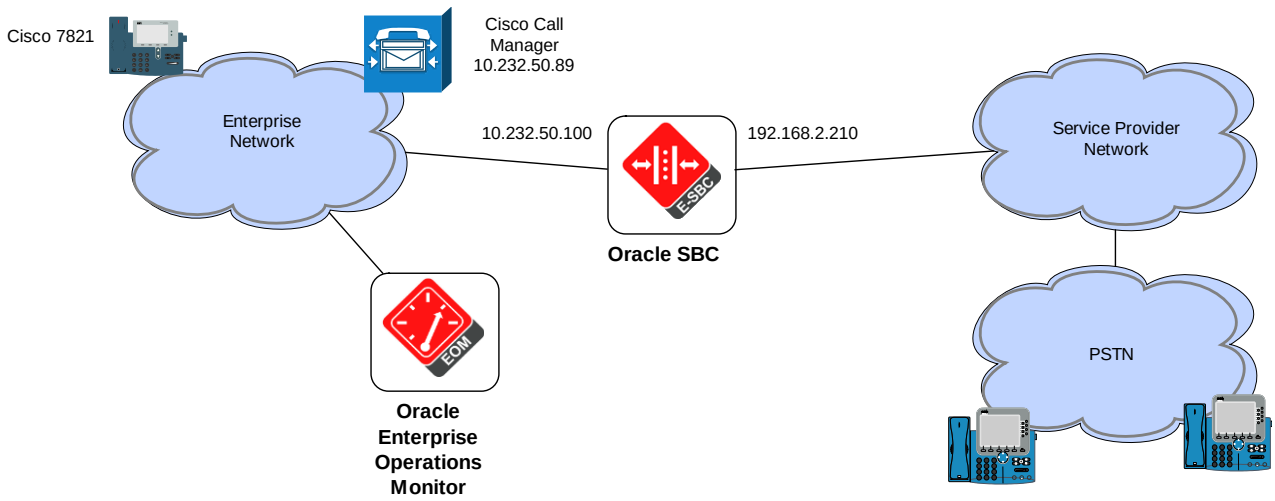
The Oracle Enterprise Session Border Controller (E-SBC) is an enterprise-class signaling component designed to simplify communications networks. It connects disparate IP communications networks while mitigating security threats, curing interoperability problems and ensuring reliability.

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

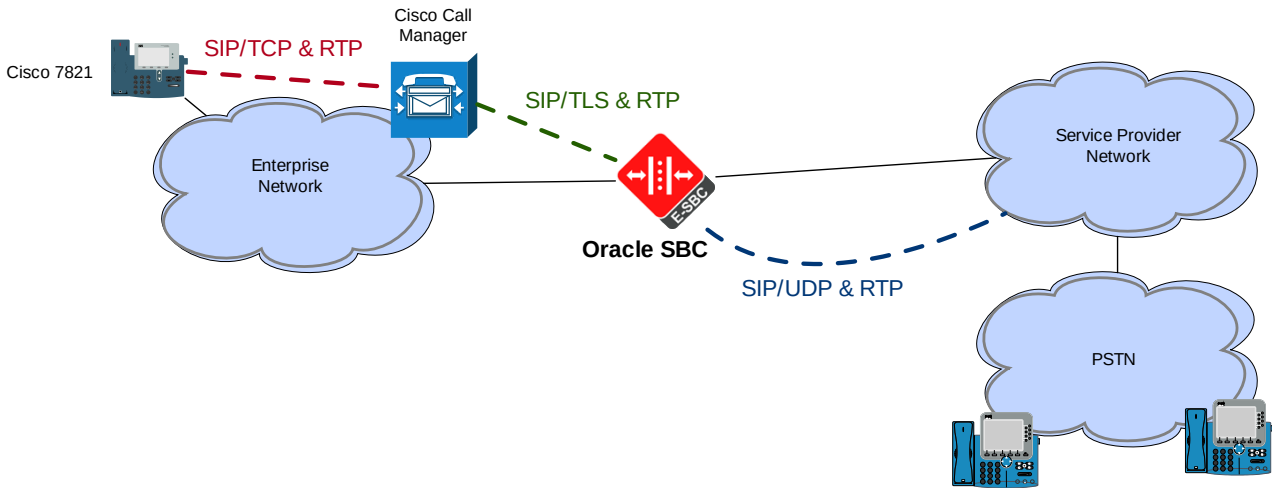
Lab Configuration

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.


Cisco Call Manager
Cisco 7821
SIP/TCP & RTP
SIP/TLS & RTP
Enterprise Network
Service Provider Network
E-SBC
Oracle SBC
SIP/UDP & RTP
PSTN

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.

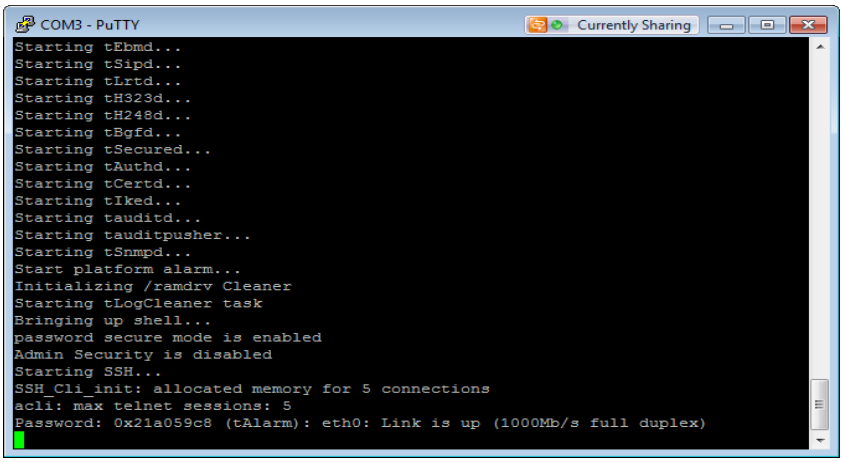
All commands are in bold, such as **`configure terminal`**; parameters in bold red such as **oraclesbc1** are parameters which are specific to an individual deployment. Only non-default parameters are shown. **Note:** The CLI is case sensitive.

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.



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

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

You are now in the global configuration mode.

Initial Configuration – Assigning the Management Interface an IP Address

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

oraclesbc1# configure terminal --> bootparam

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

```
oraclesbc1(configure)# bootparam

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

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

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

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

Configuring the 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 <certficate-record-name>" command, where the certificate is pasted into the Command Line Interface (CLI) after issuance of the command, followed by a semi-colon (";") to indicate the end of the certificate, and then a save/activate. Here is an example of the certificate importation process after the corresponding certificate-record has been configured and a save/activate has been performed.

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

IMPORTANT:

Please enter the certificate in the PEM format.

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

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

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

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

Generating the SBC's Certificate Signing Requests

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

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

generate-certificate-request ExampleSbcCertA

Generating Certificate Signing Request. This can take several minutes....
-----BEGIN CERTIFICATE REQUEST-----
MIIByTCCATICAQAwXjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEXMBUGA1UEAxMOMTky
LjE2OC4xMy4xMTMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANoAWTk8tHzE
tblCL88CFwx9s9soqbKr0u+ZSJQEKsV0OUMtPX60X5+Z94TORp1waZMcSTSHktmR
OrUsF8j9OV/5YvCJFWxvxMXOpivdO9Tbd7M44776P41weIBRXNBv7aWv2qzc4gUx
IFXRcf4xBnyZllLxEwO68ezZxB3y8EUNAgMBAAGgKzApBgNVHQ8xIhMgZGlnaXRh
bFNpZ25hdHVyZSxrZXlFbmNpcGhlcm1lbnQwDQYJKoZIhvcNAQEFBQADgYEAcSZH
6nig6A2GgAnCTUTjraJH/bMHoFQkeXOWcmUf84u6VKyV/9EDhlE/hdjG5/32KIXP
d6zQ7J9GeanvrkSqa757rI2uqbRR/cQlWPNGAG4TocNwdkZznGYm9Du4qPH4ceSh
stD/bBql63NjkSKrQXwpB6VZYfcATH6X++7VRco=
-----END CERTIFICATE REQUEST-----

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

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

Importing the SBC's Signed Certificates

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

Managing Certificate Expirations to Avoid Service Disruptions

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

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                                    s1p0
        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                                    s1p0
        operation-type                          Media
        slot                                    1
```

Realm Configs

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

```
realm-config
        identifier                              cisco-core
        network-interfaces                      s1p0:0
        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.

```
oraclesbc1# save-config
checking configuration
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbc1# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbc1# reboot force
```

The E-SBC configuration is now complete.

Phase 2 – Configuring the Oracle Enterprise Operations Monitor

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

In Scope

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

Out of Scope

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

What will you need

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

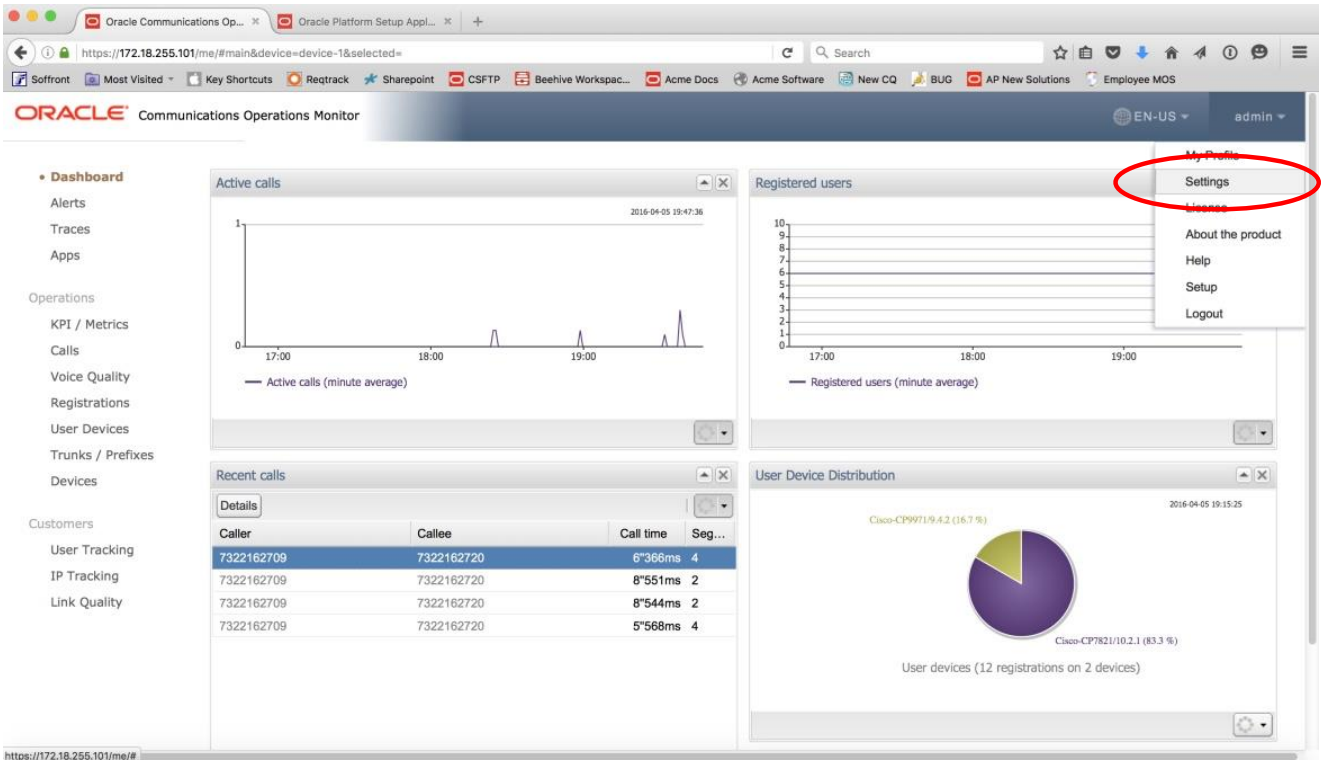
EOM – Getting Started

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

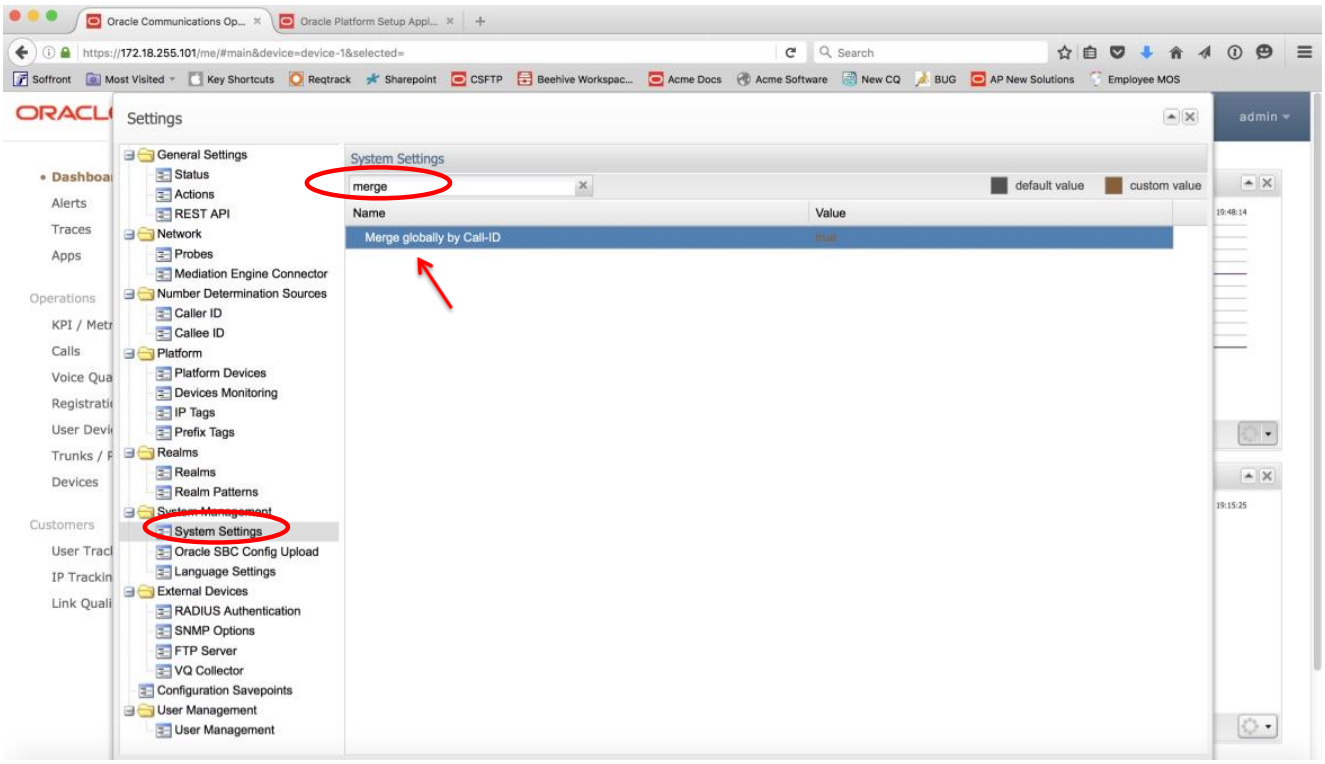
Configuring EOM to Display All Legs of a Call in a Single Report

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

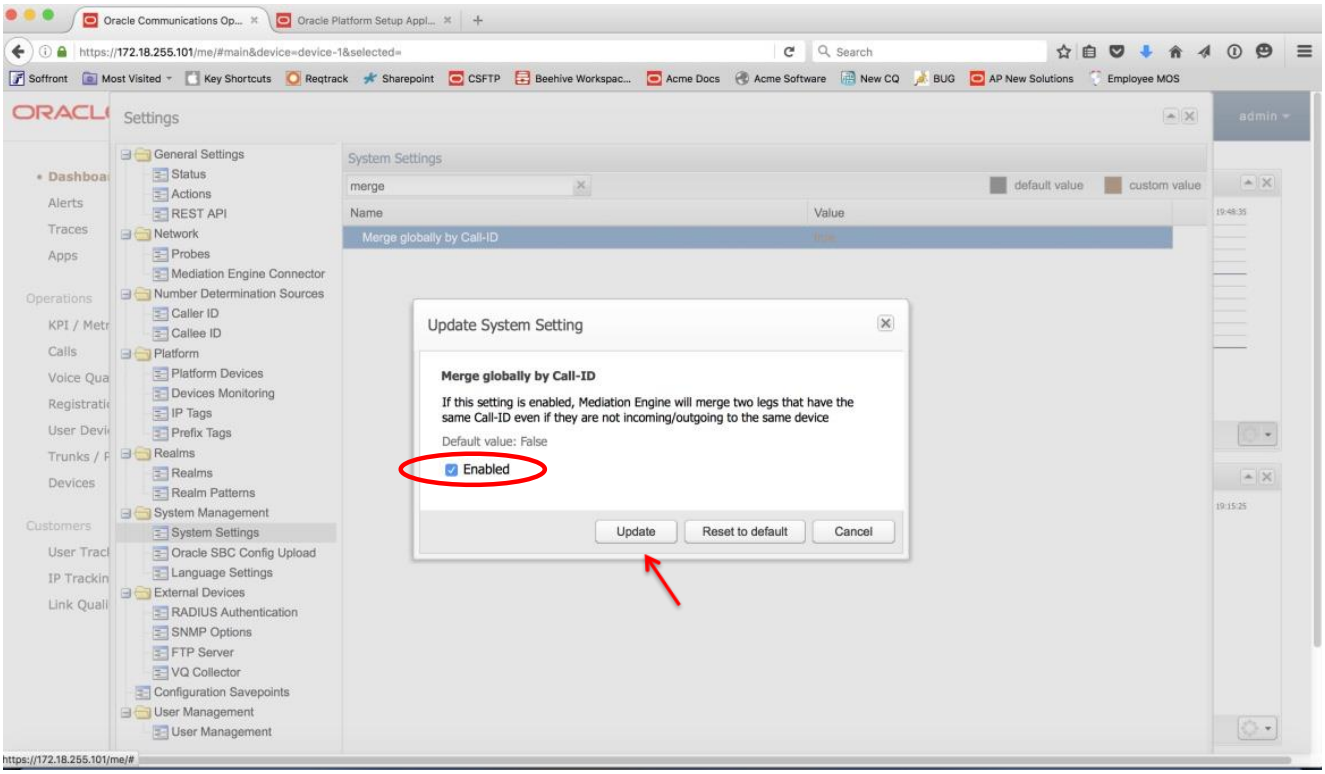
1. Click on the user (admin in this example) in the top right corner, then click on Settings.



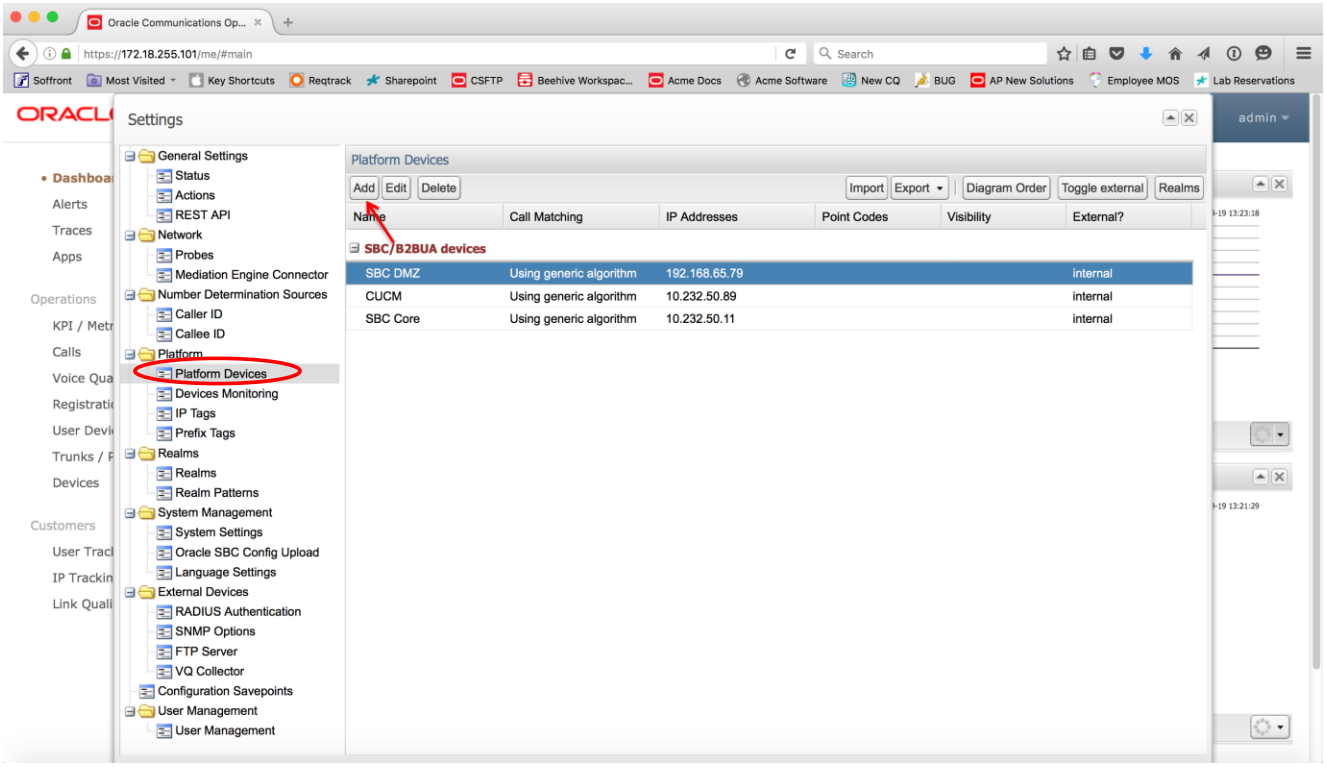
2. Under System Management select System Settings and search for “merge”. Double click on “Merge globally by Call-ID”.



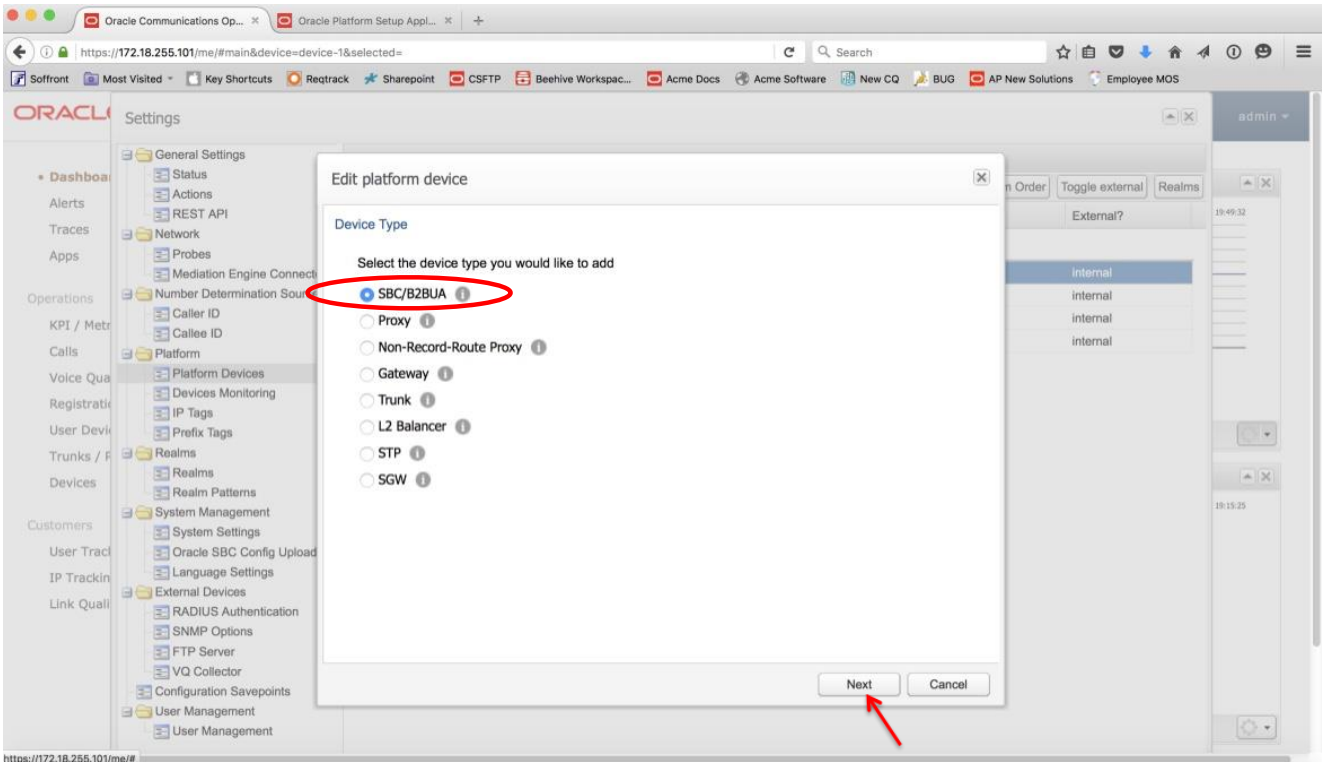
3. Click on the Enabled check box and click Update.



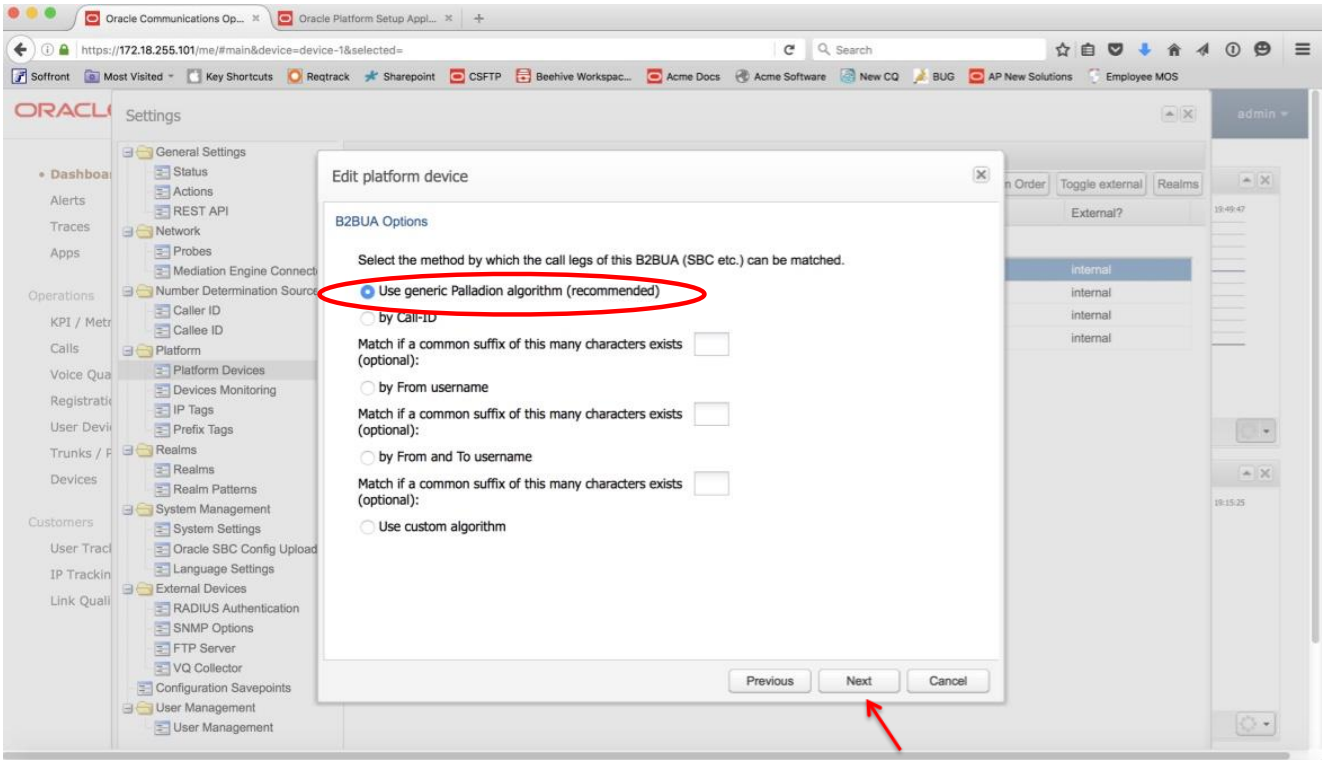
4. Under Platform select Platform Devices. Click Add (or Edit if you've already added a device).



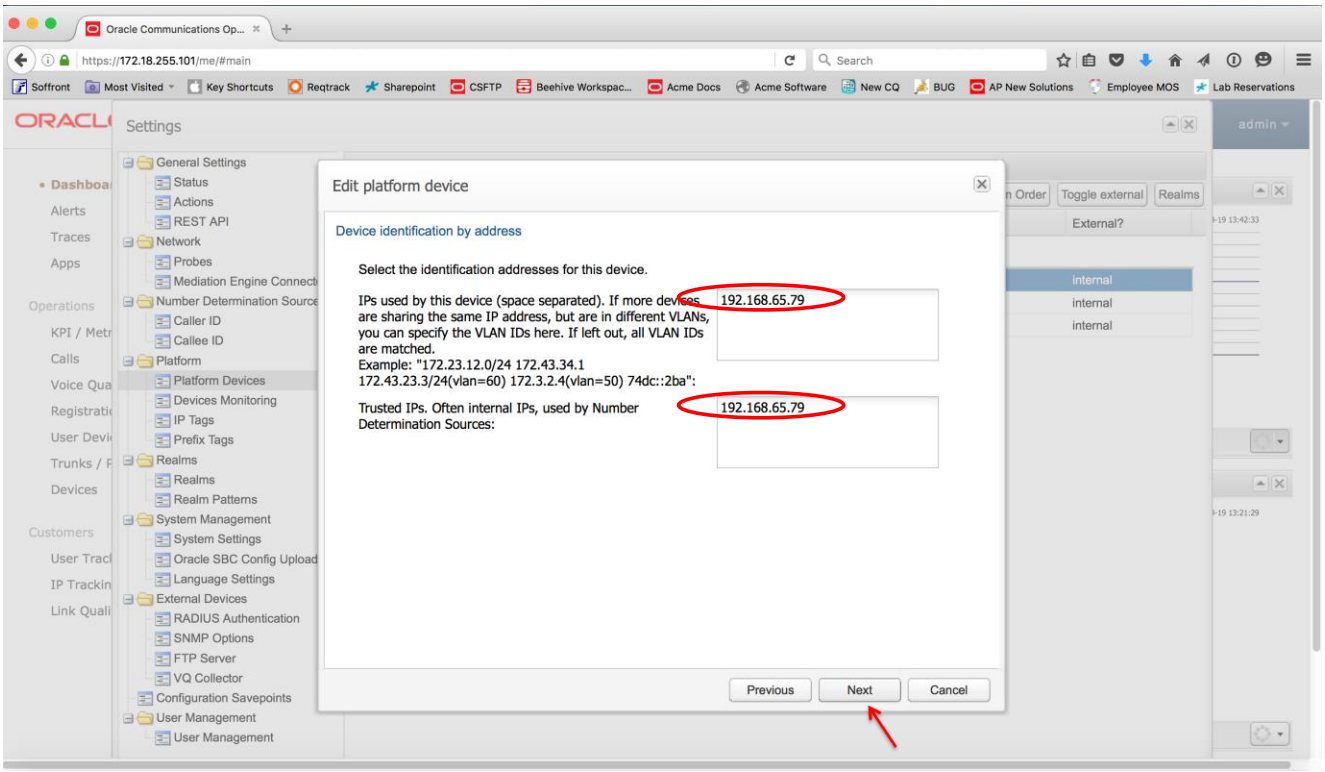
5. Select the SBC/B2BUA radio button regardless of the type of device you're adding, then click Next.



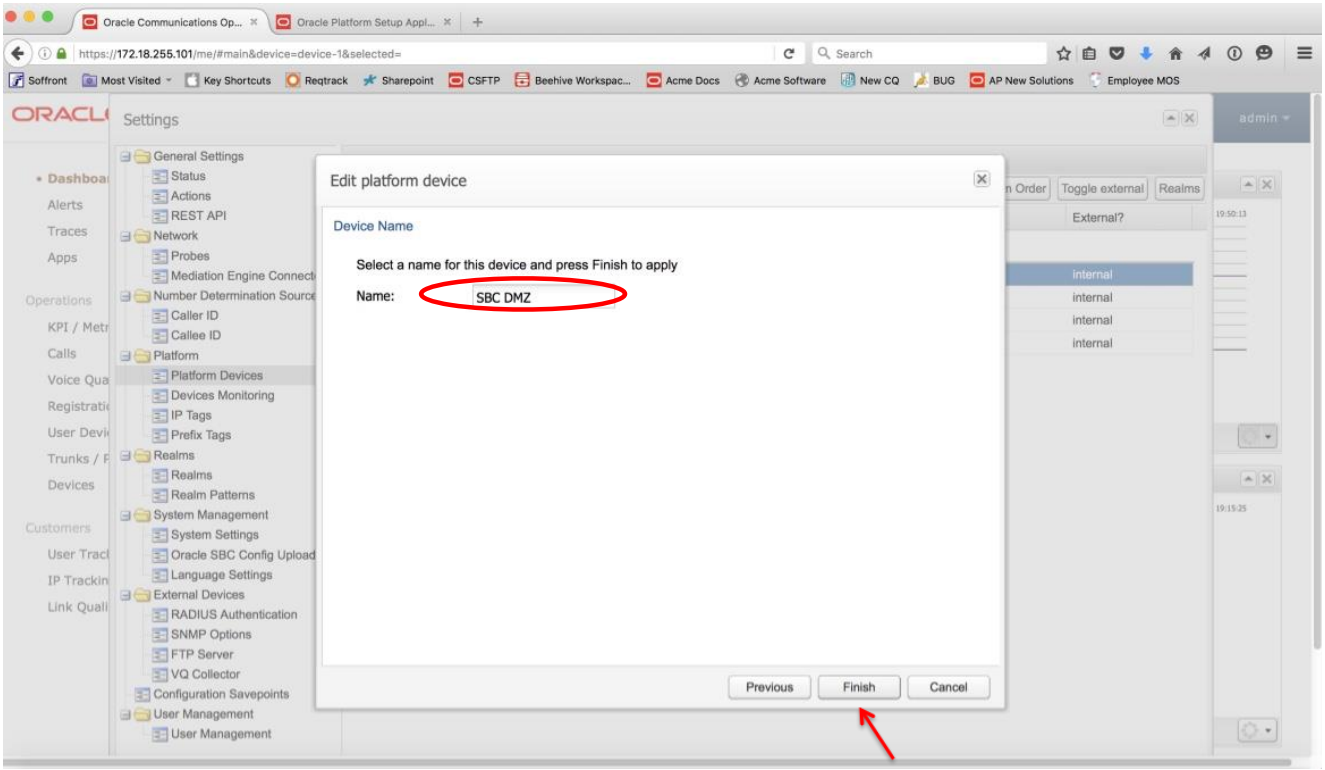
6. Click on the “Use generic Palladion algorithm (recommended)” radio button, then click Next.



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

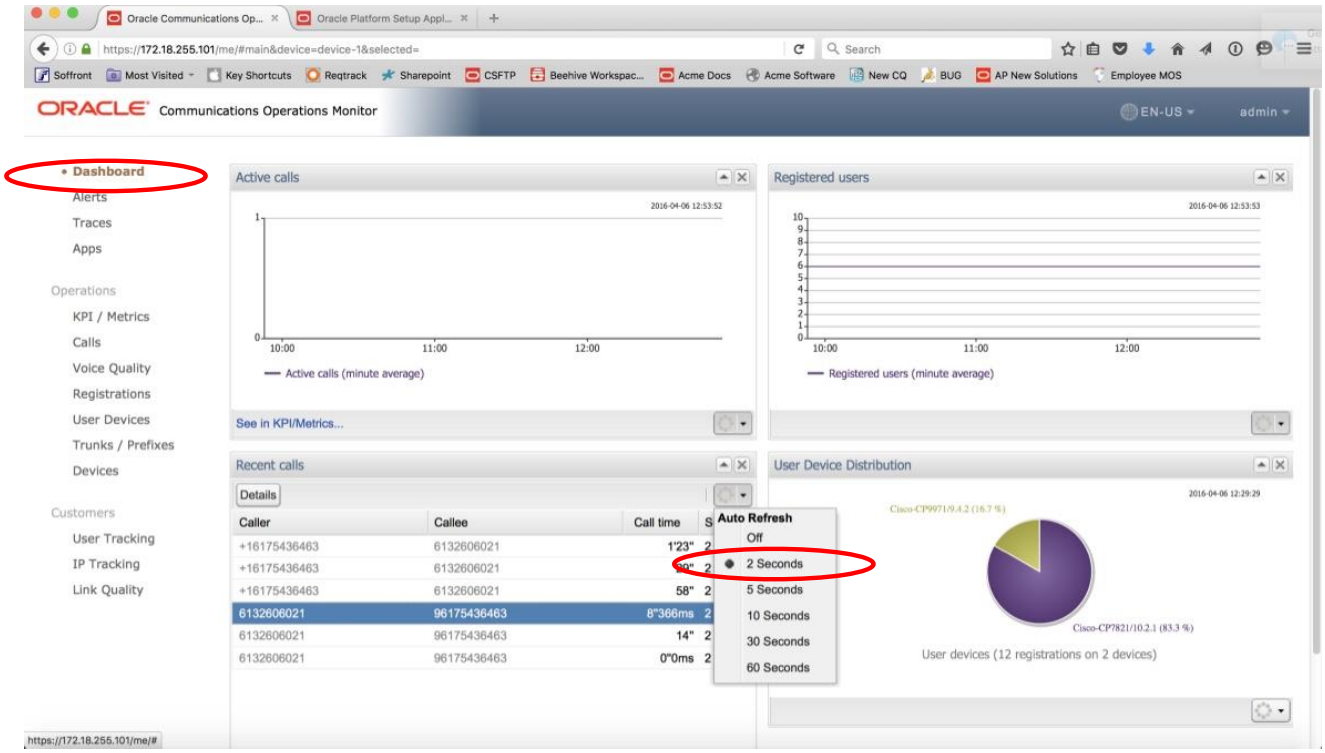


8. Enter a name for the device and click Finish.

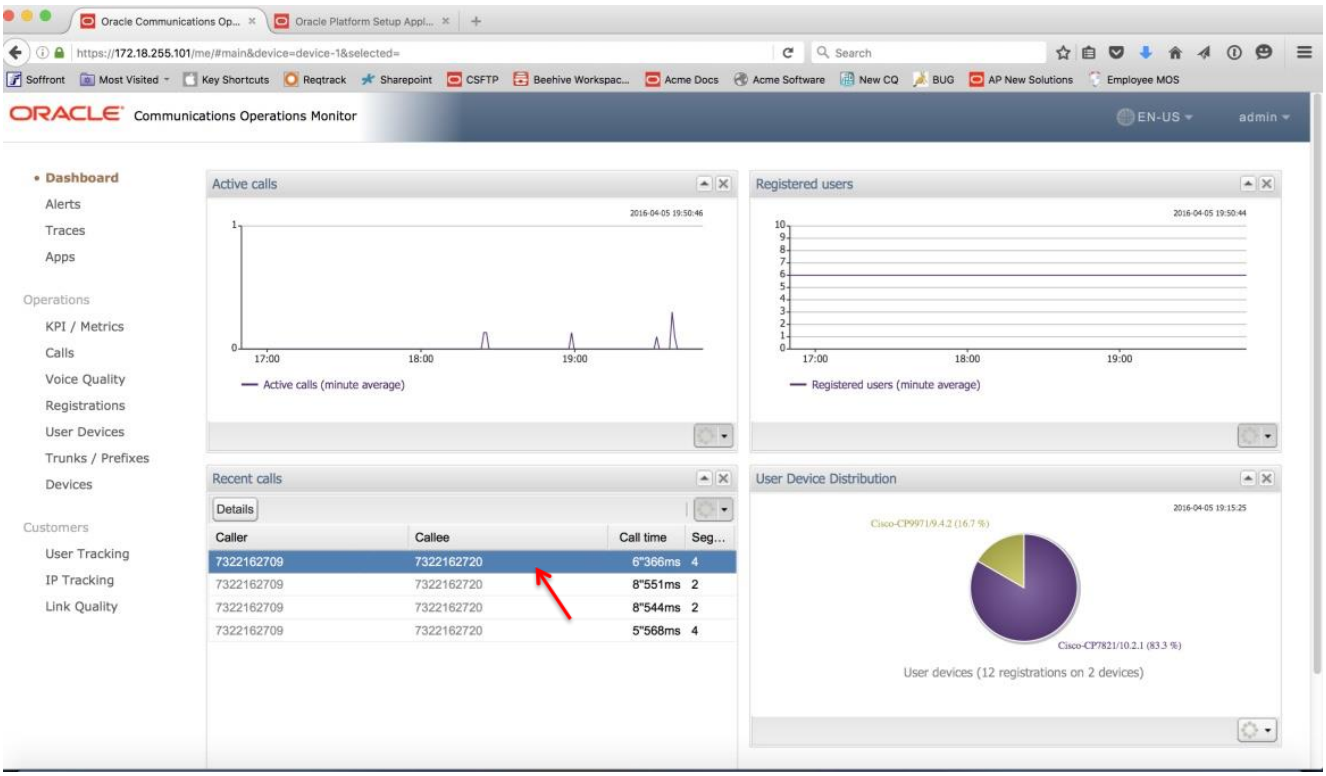


9. Repeat for all other devices in the call flow. Enter each side of the SBC (inside and outside) separately.

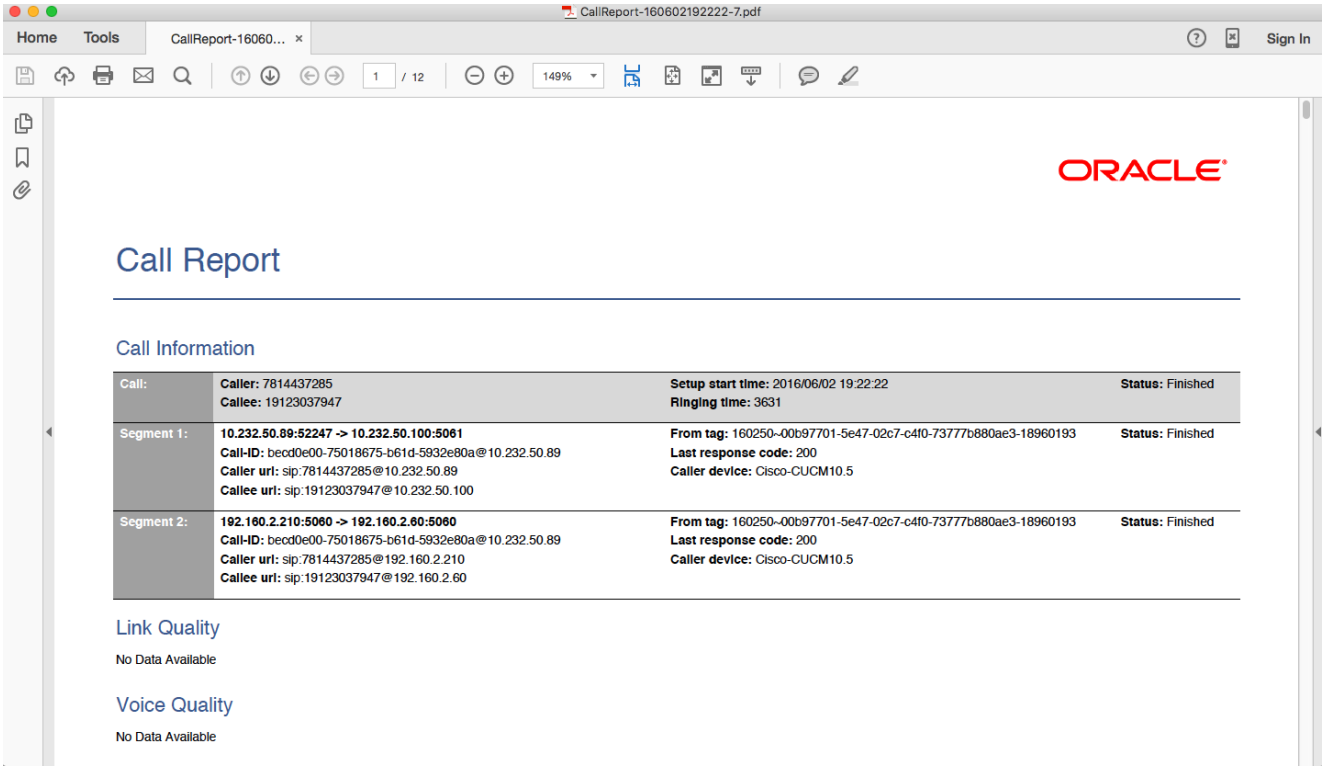
10. On the Dashboard, under Recent Calls, make sure the Auto Refresh is set to something other than Off.



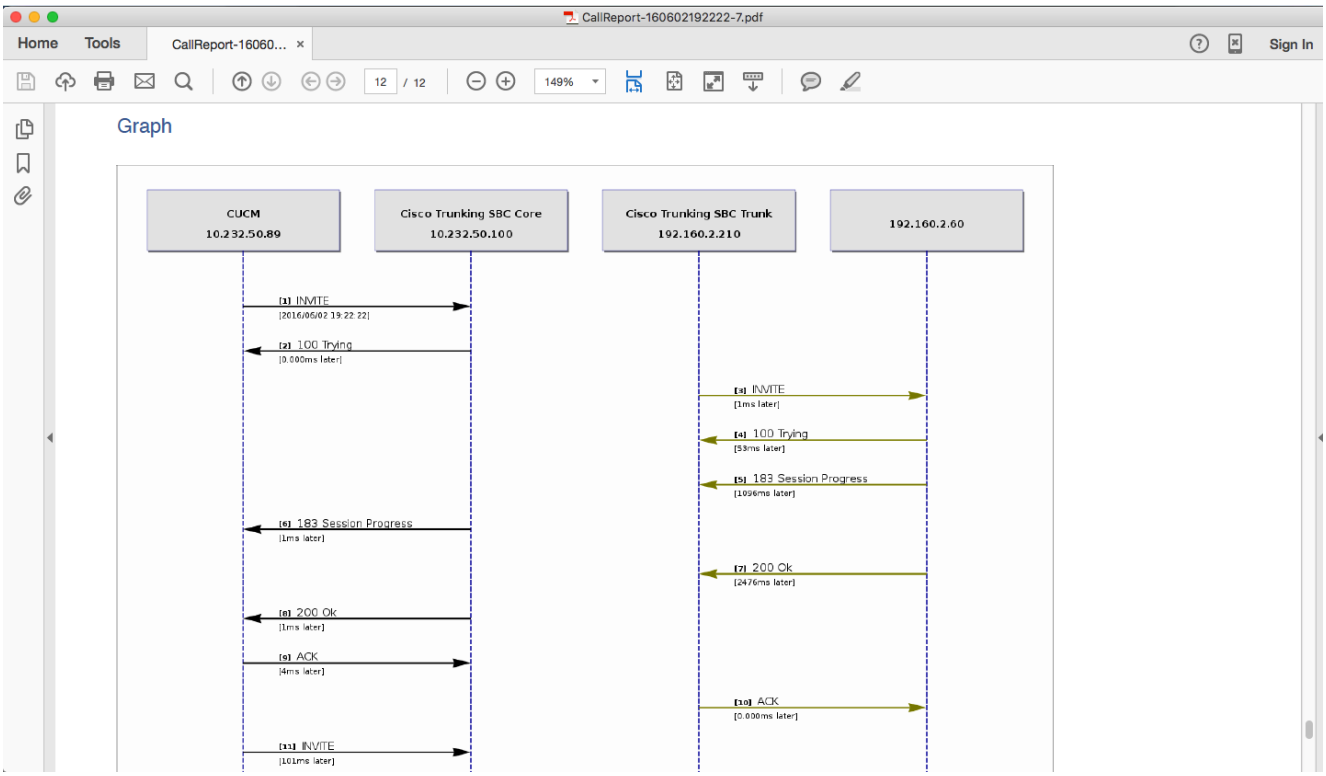
11. Make a call. After the call is finished, the call will show up under Recent Calls with 2 or more segments if the call only traverses the SBC once, or with 4 or more segments if the call traverses the SBC twice. Double click on the call.



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



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



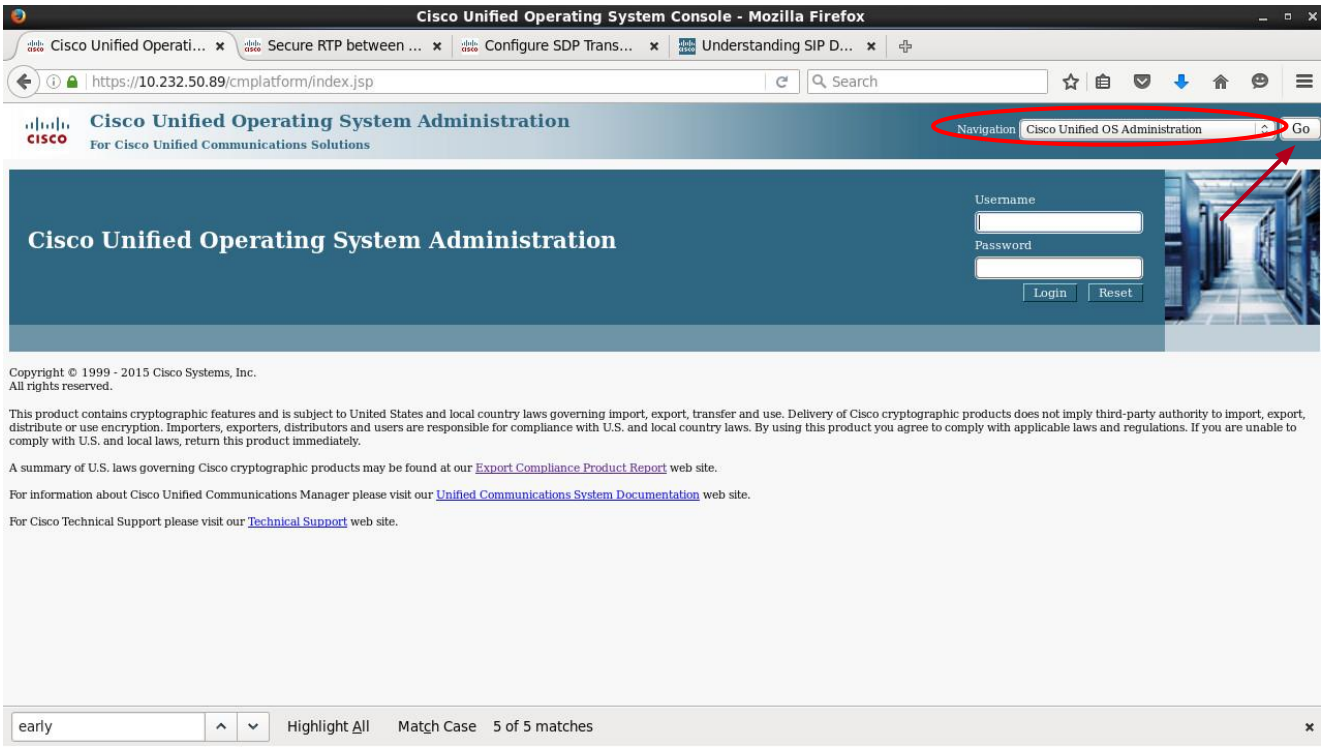
Phase 3 – Configuring the Cisco Unified Communications Manager (CUCM)

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:

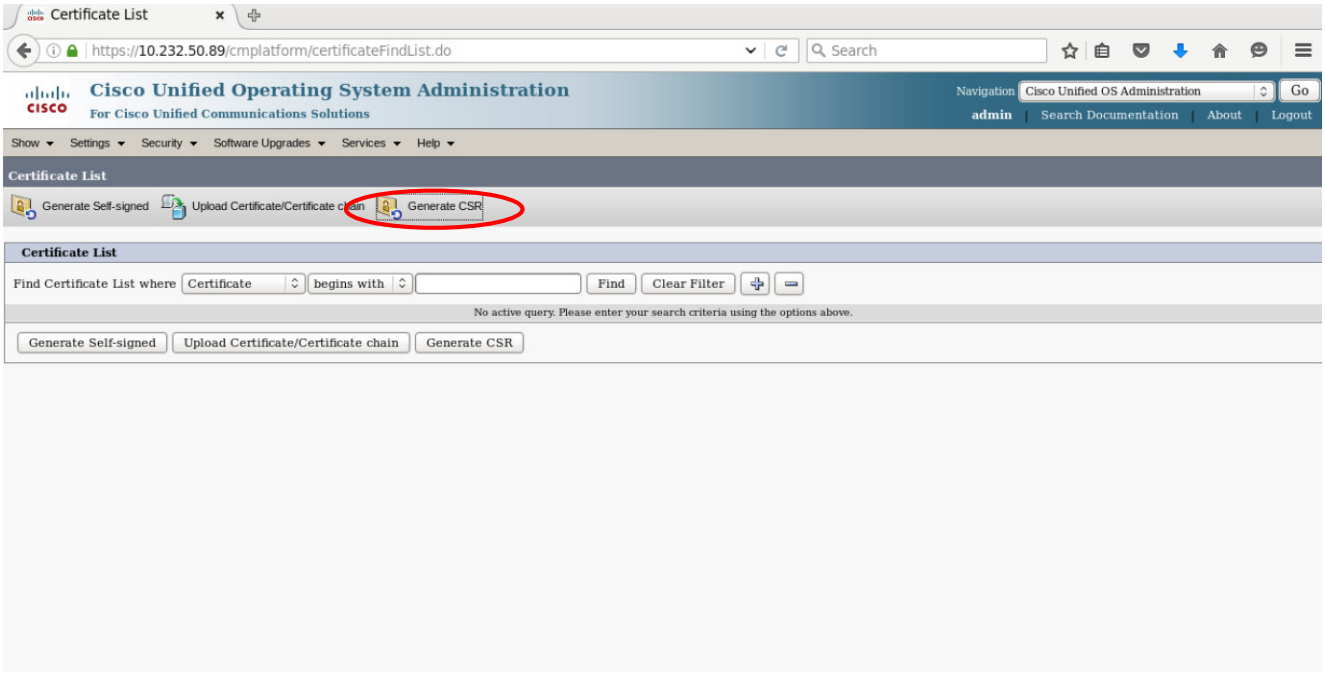
- Generating a Certificate Signing Request (CSR) for CallManager
- Importing the Certificate Authority (CA) certificate
- Importing the CallManager certificate signed by a CA
- Configuring a SIP Trunk Security Profile
- Creating a SIP Profile
- Configuring a SIP Trunk
- Creating a Route Pattern
- Setting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

Generating a Certificate Signing Request (CSR) for CallManager

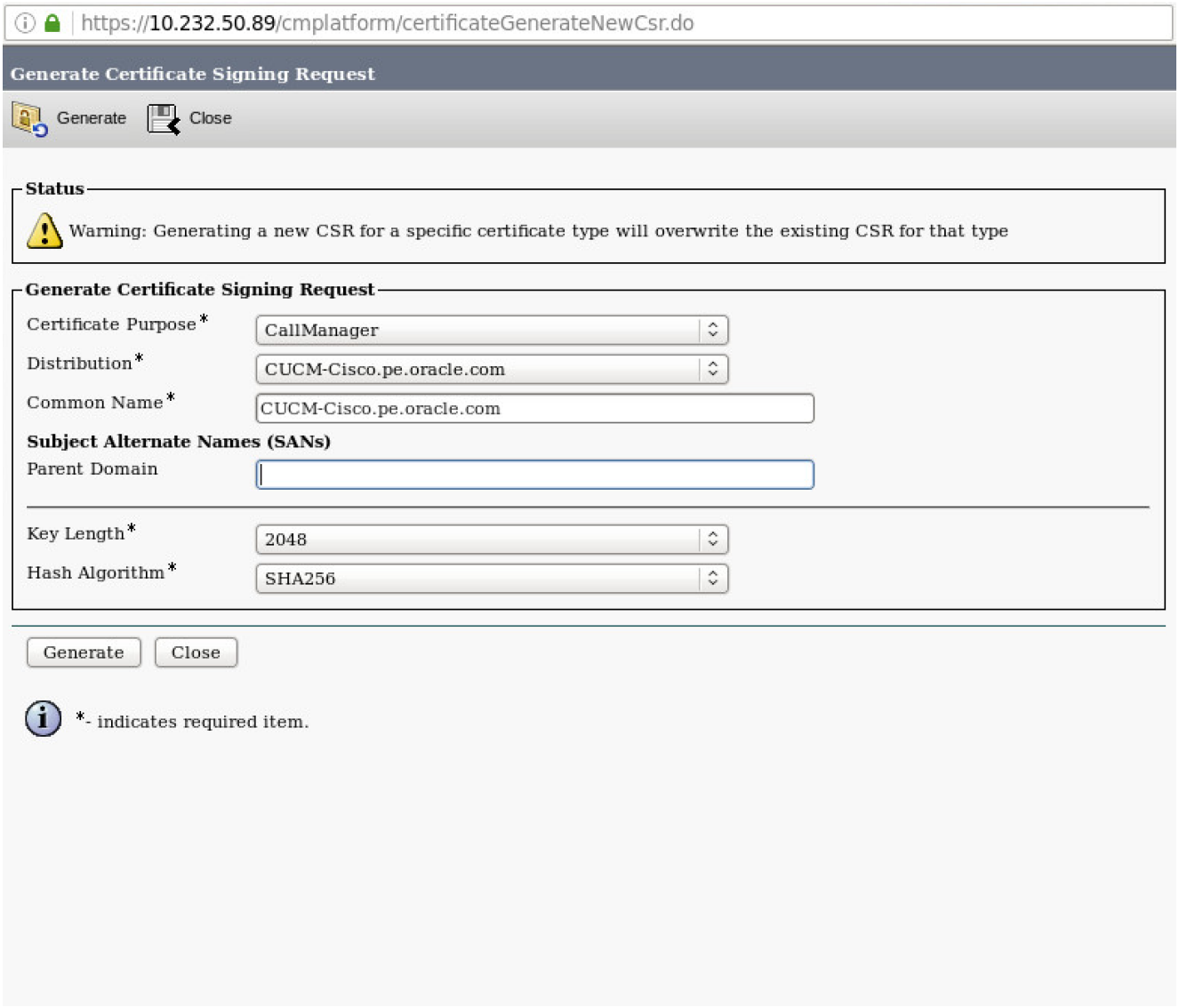
Log in to the Cisco Unified OS Administration.



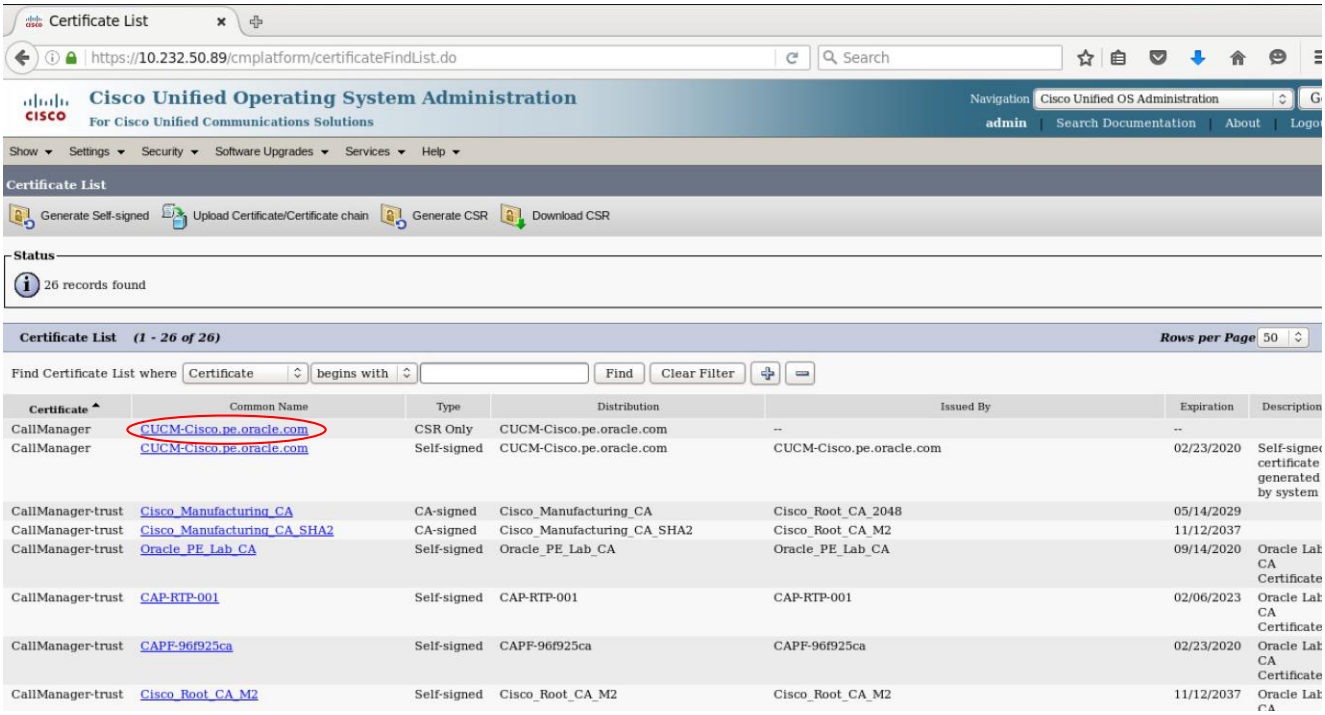
Click on Generate CSR.



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.

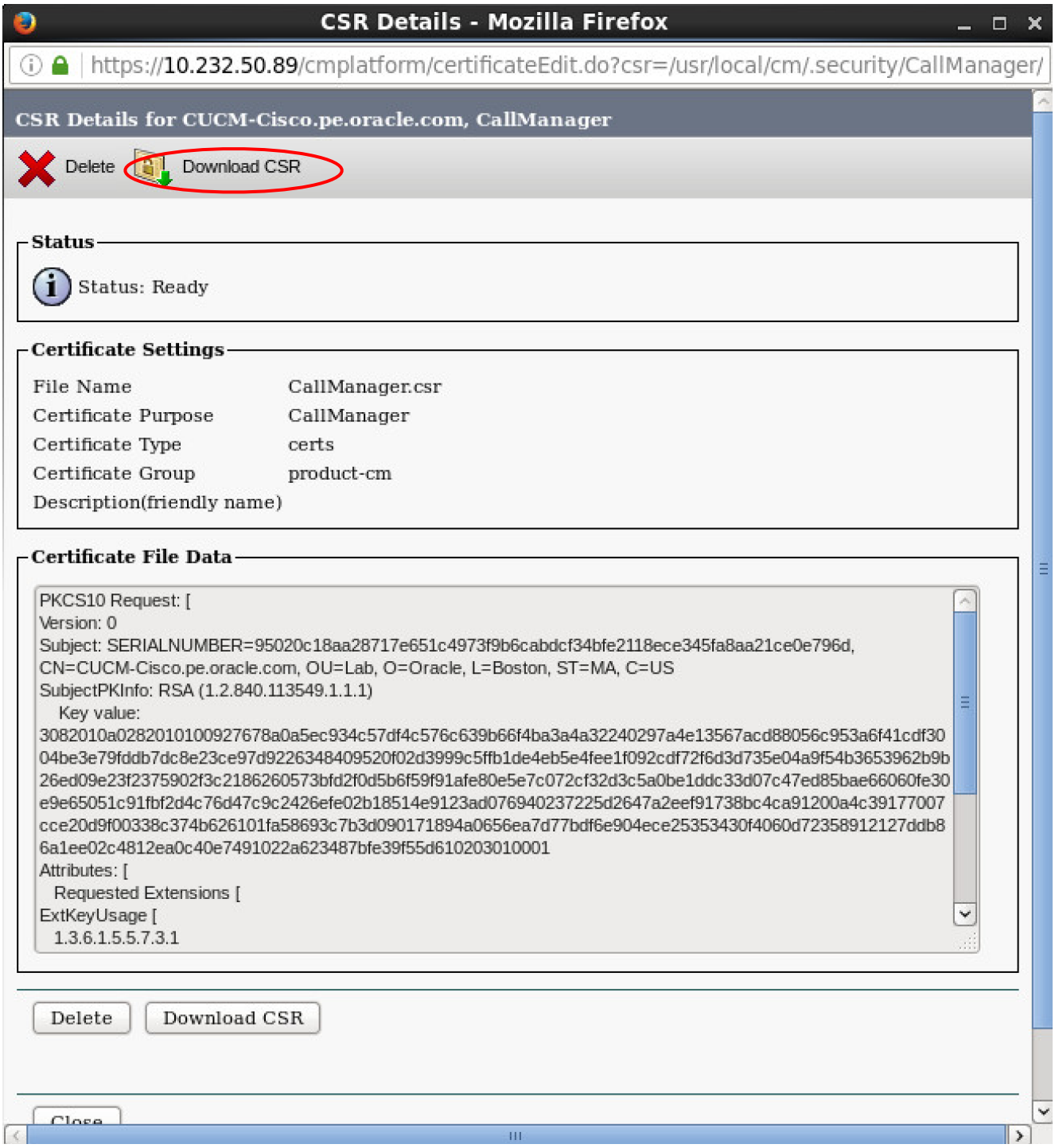


You will see a list of certificates. Click on the FQDN that has “CSR Only” listed as the type.

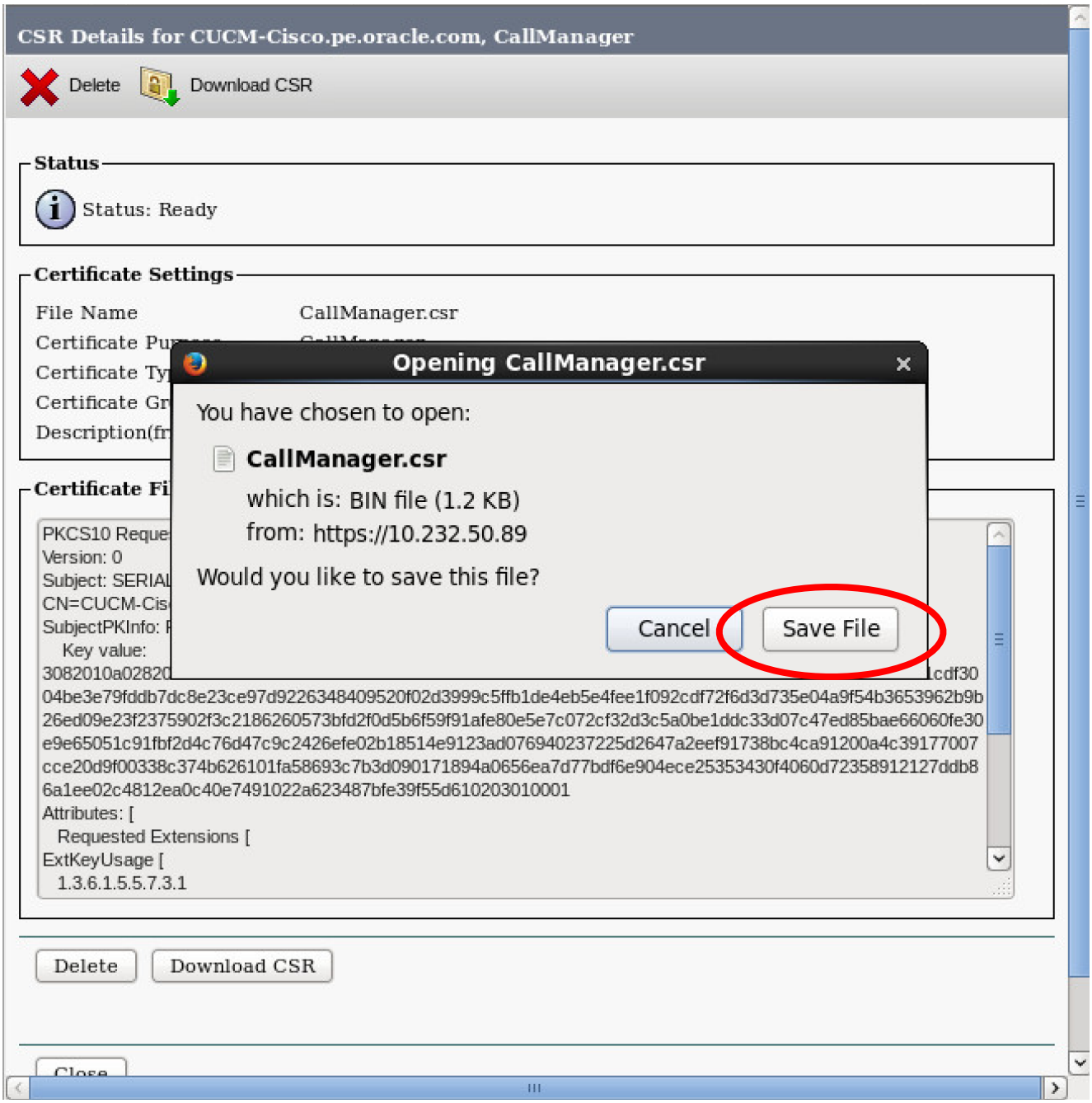


Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM-Cisco.pe.oracle.com	CSR Only	CUCM-Cisco.pe.oracle.com	--	--	
CallManager	CUCM-Cisco.pe.oracle.com	Self-signed	CUCM-Cisco.pe.oracle.com	CUCM-Cisco.pe.oracle.com	02/23/2020	Self-signed certificate generated by system
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.



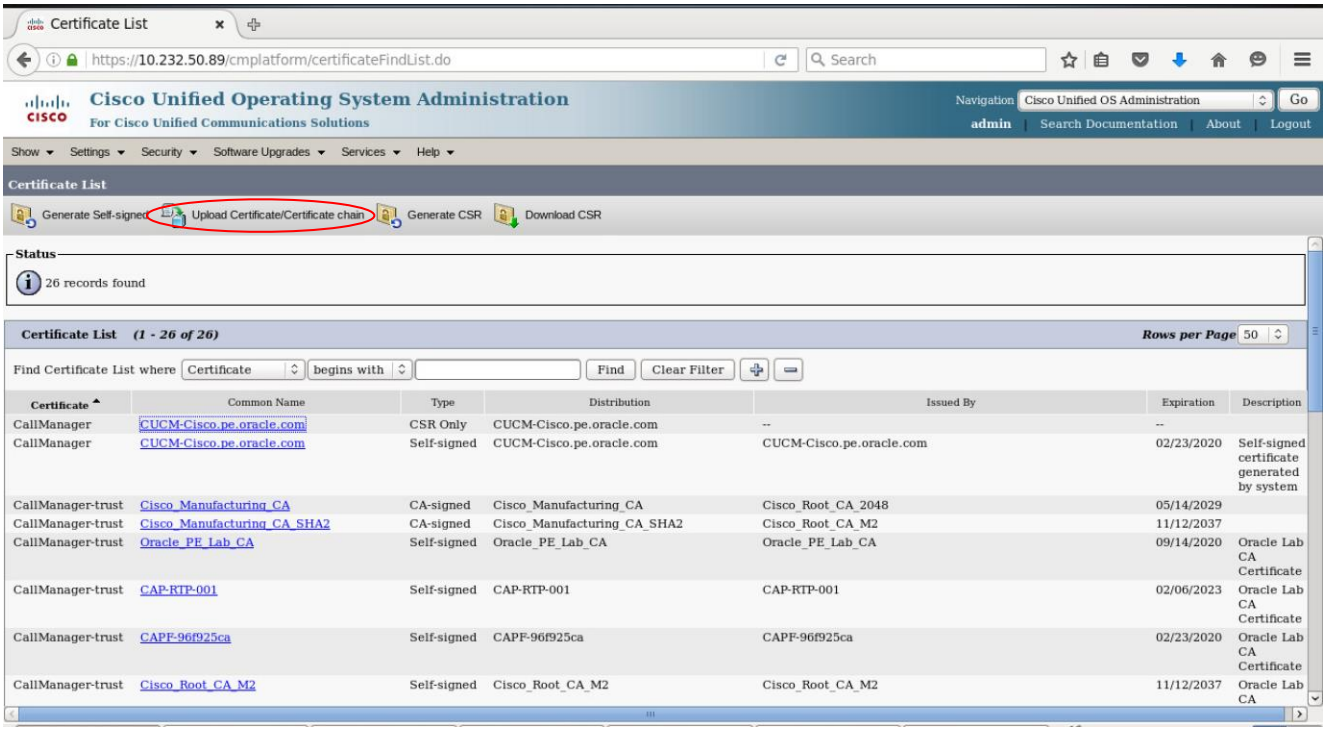
Click on Save File and save the file to your PC or server.



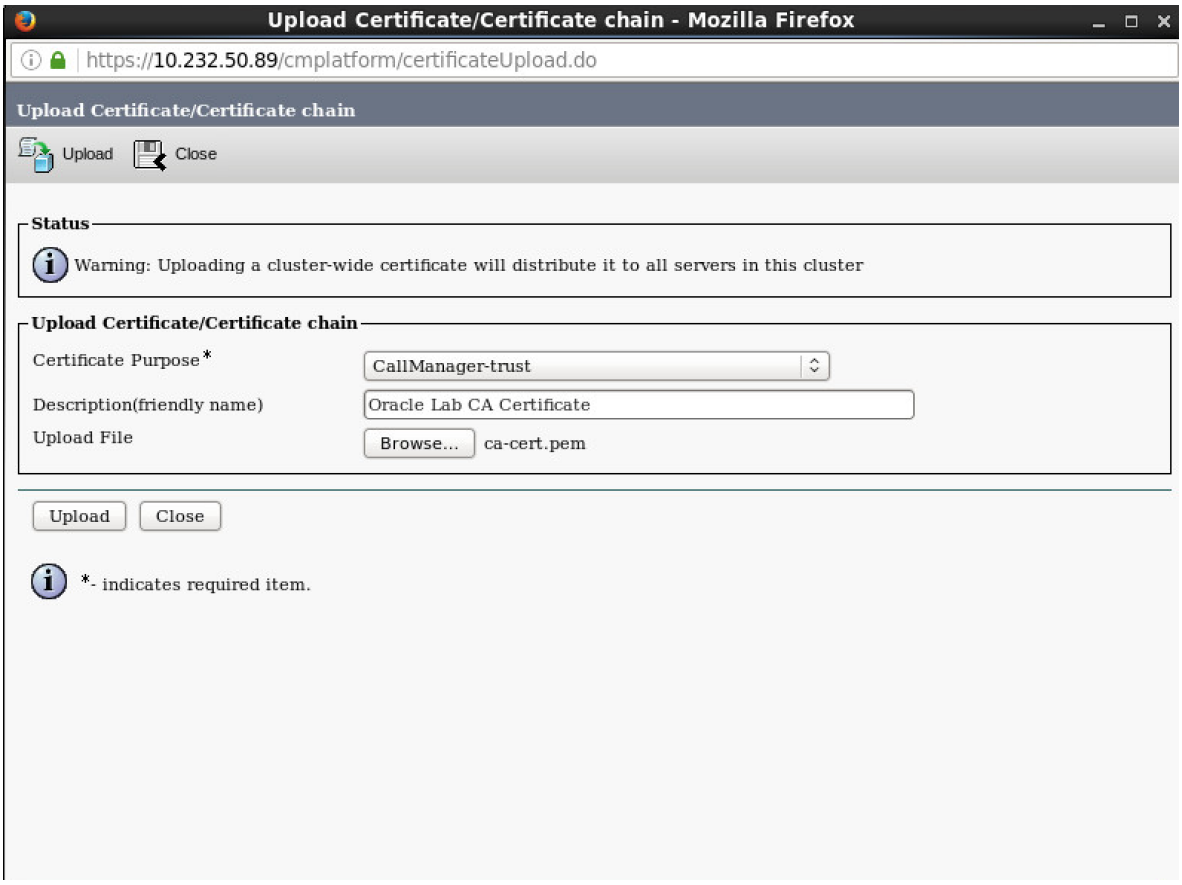
Send the CallManager.csr file to your Certificate Authority to be signed.

Importing the Certificate Authority (CA) Certificate

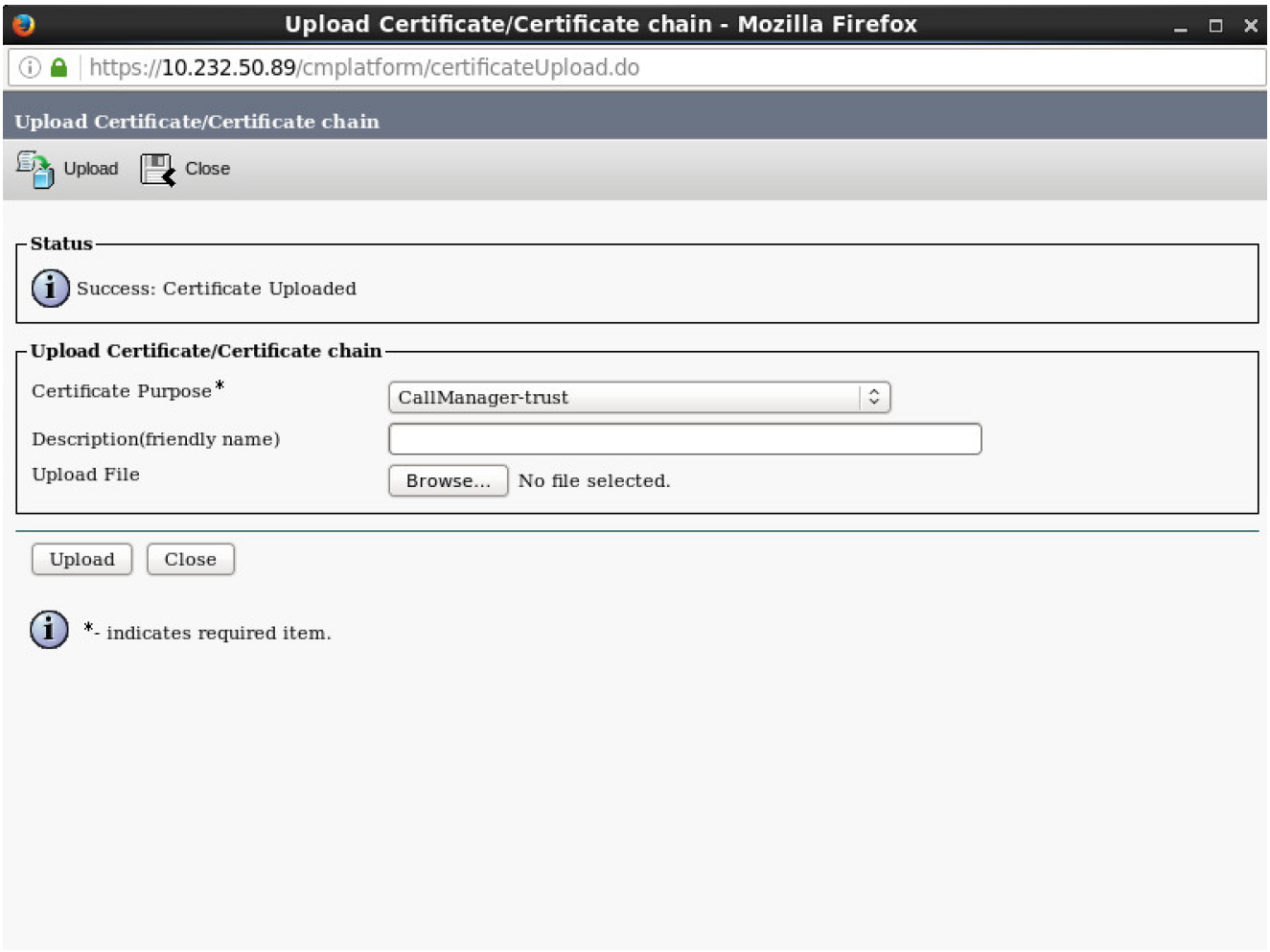
Import the Certificate Authority's (CA's) certificate in PEM format to the CallManager-trust store. Click on Upload Certificate/Certificate Chain.



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

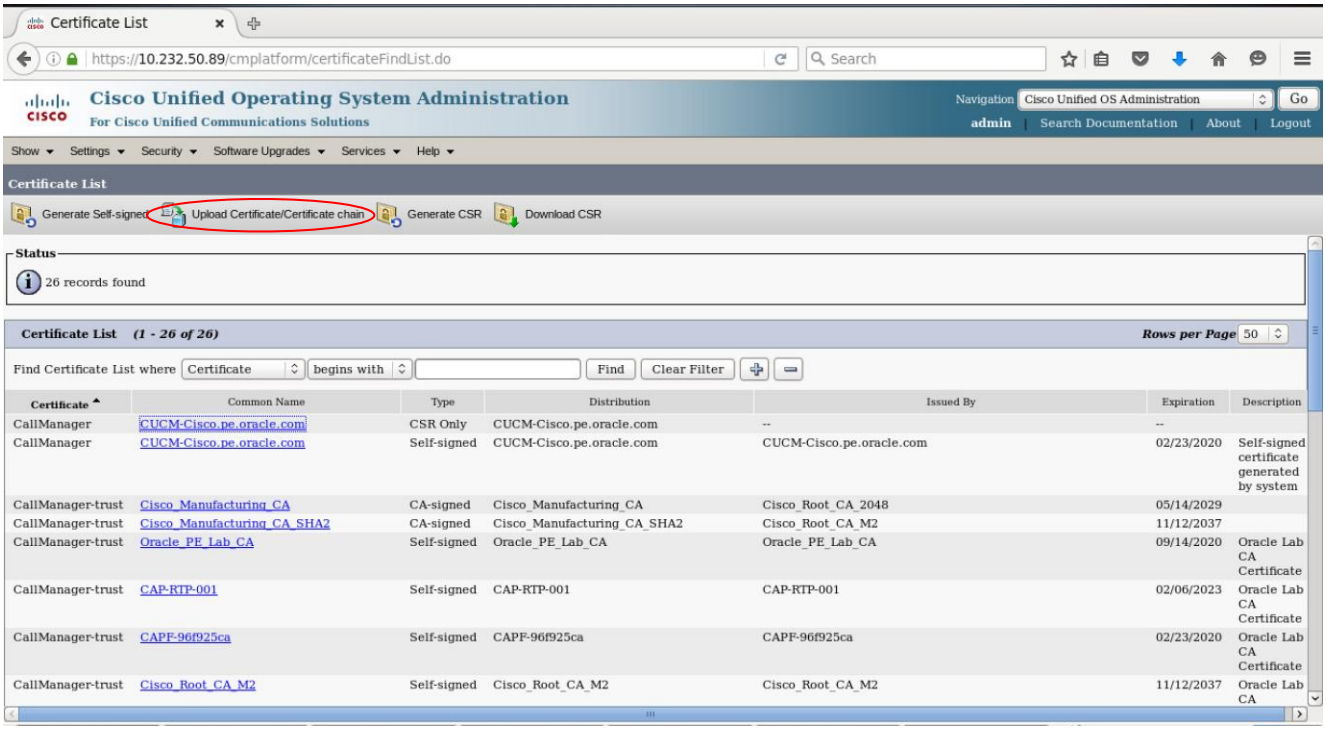


You should see “Success: Certificate Uploaded”.

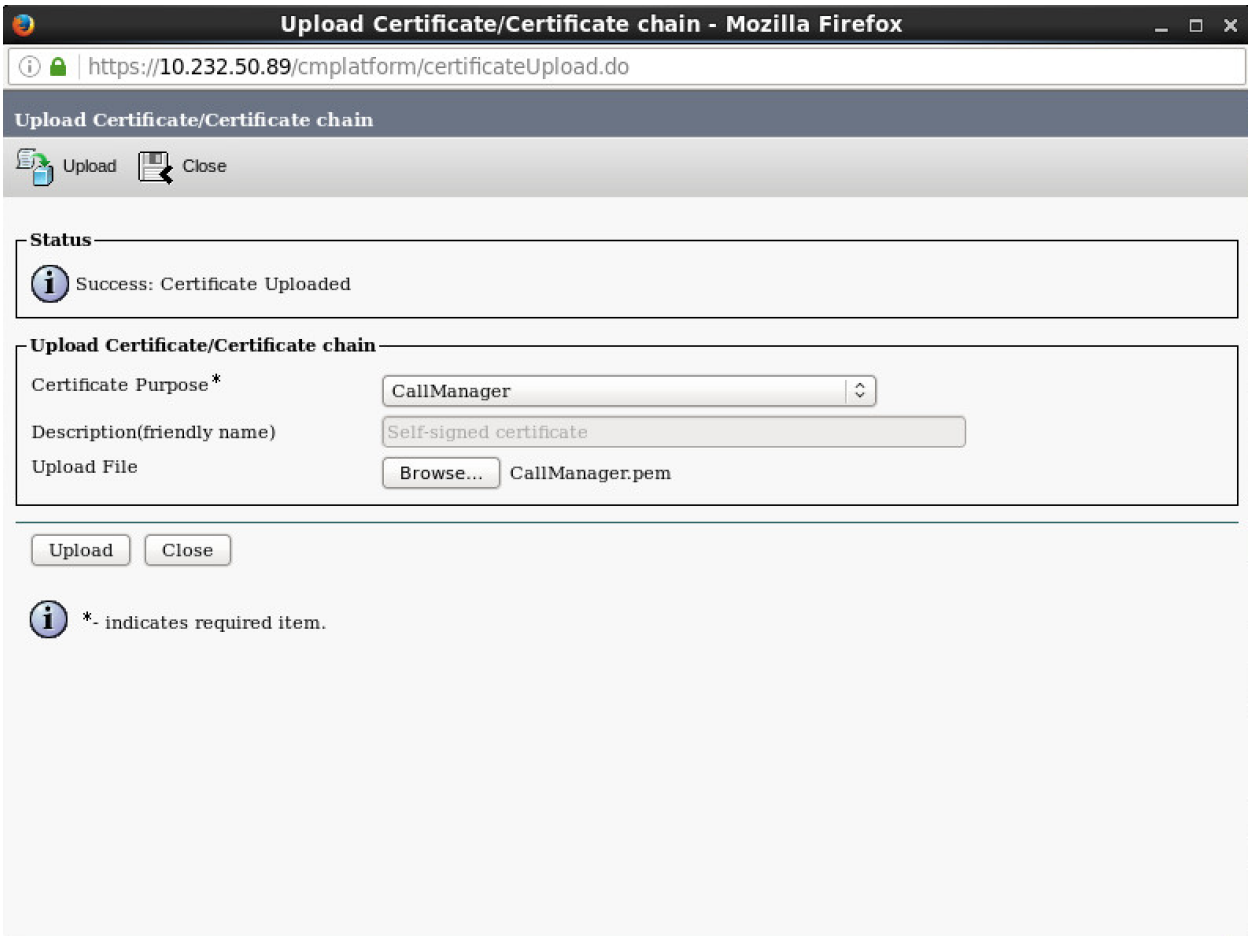


Importing the CallManager certificate signed by a CA

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



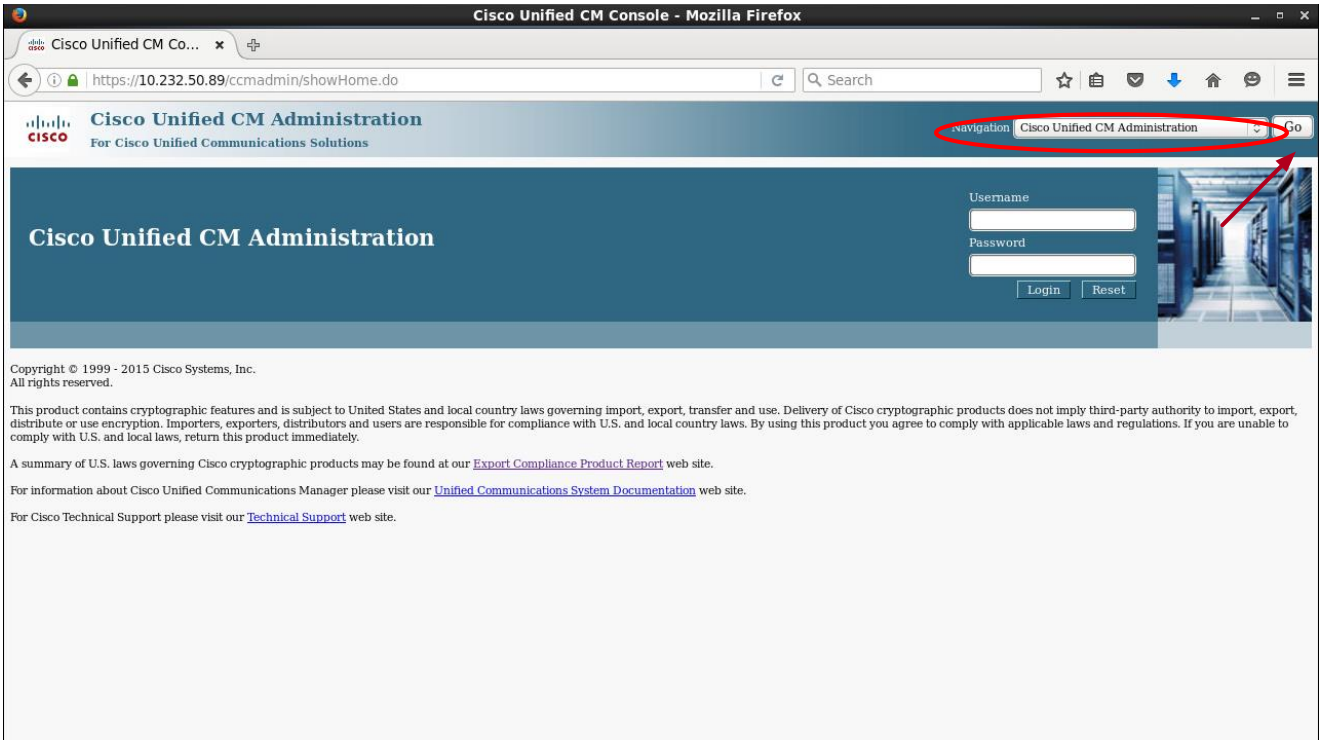
Select CallManager as the Certificate Purpose. Click Browse to find the signed certificate on your PC or server. Then click Upload.



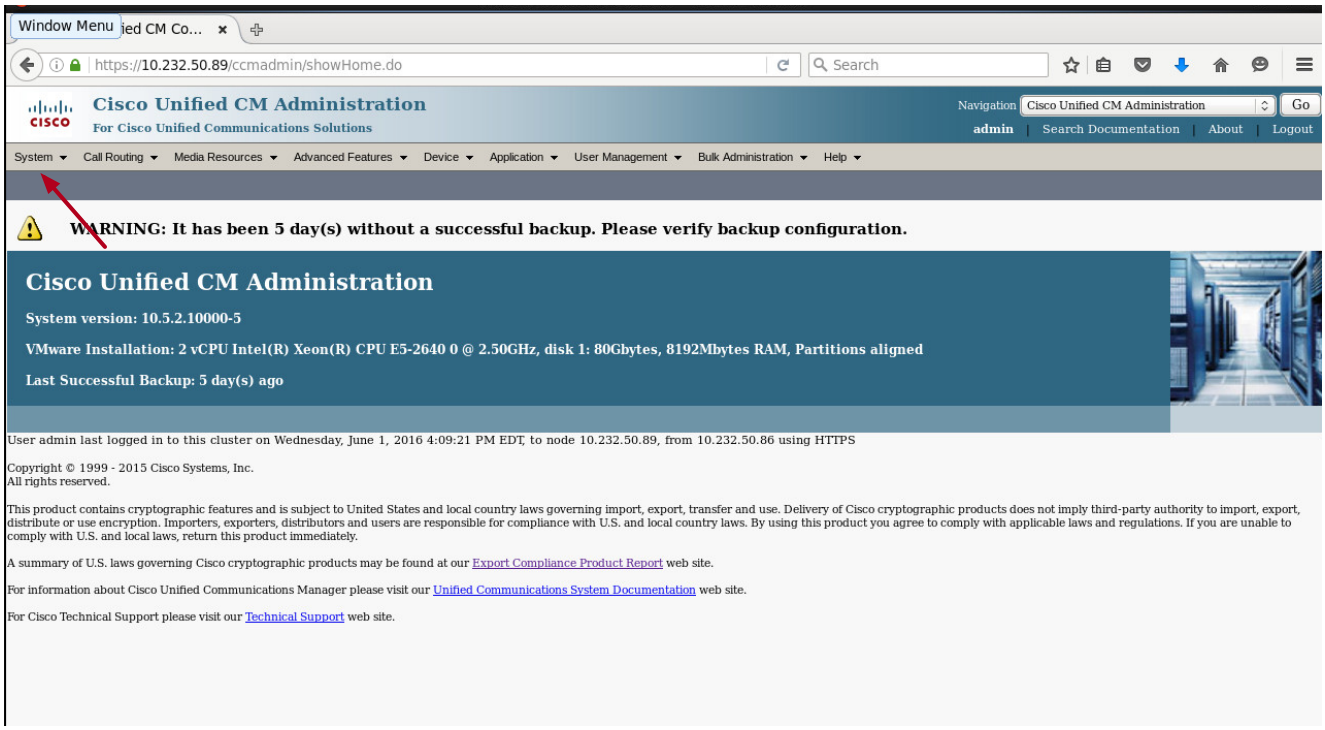
You should see “Success: Certificate Uploaded”.

Configuring a SIP Trunk Security Profile

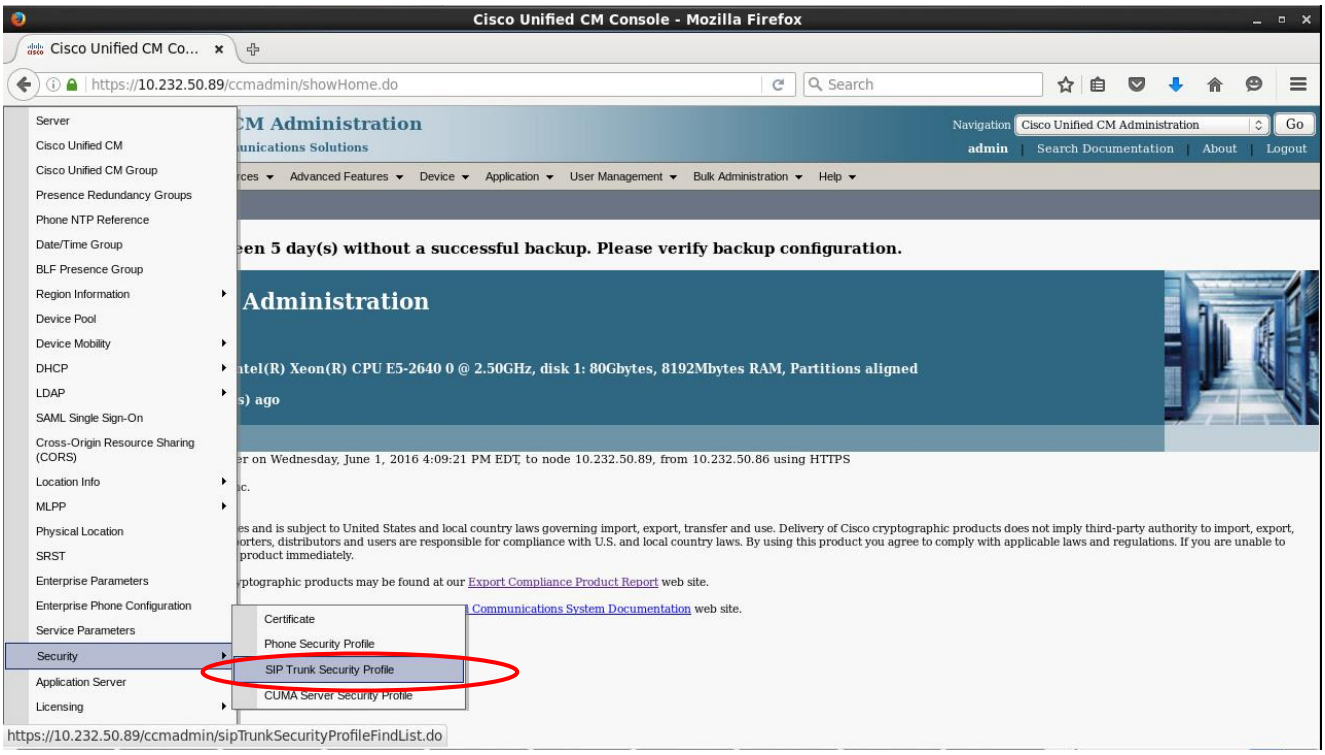
Navigate to Cisco Unified CM Administration and login.



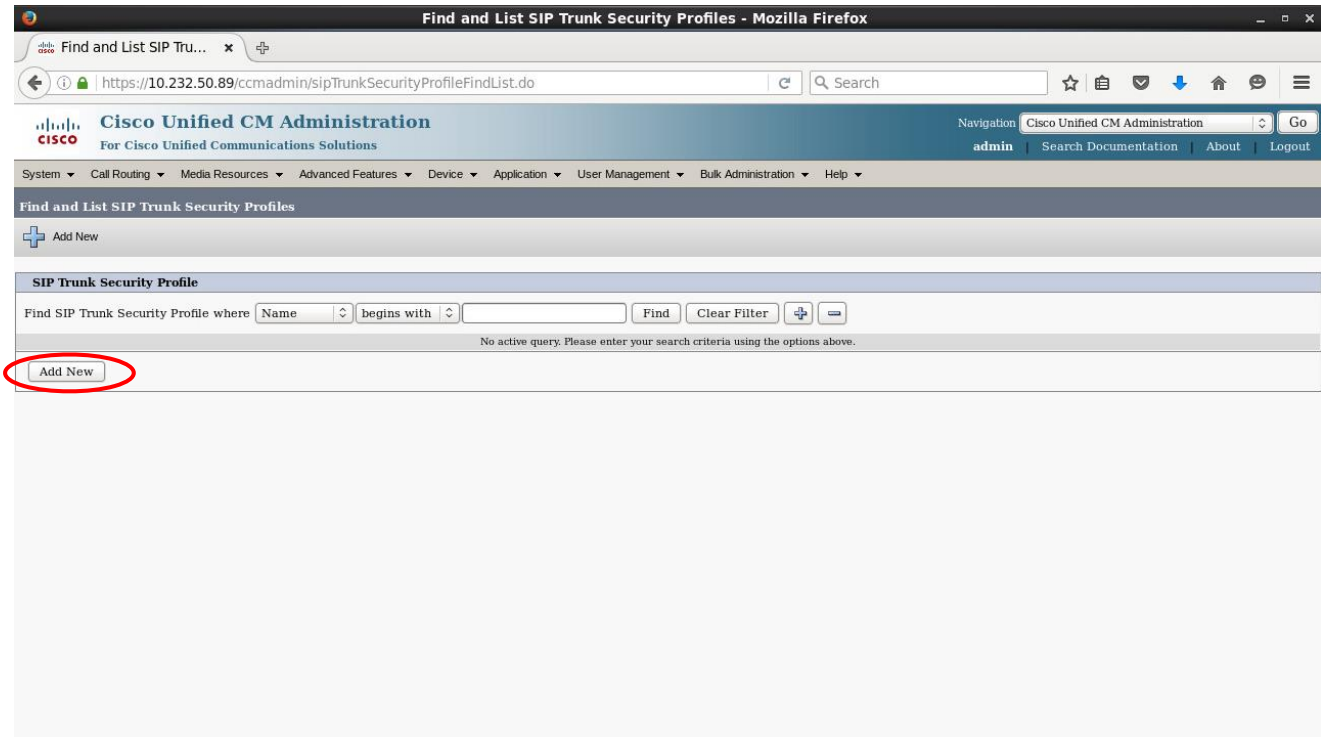
Click on System.



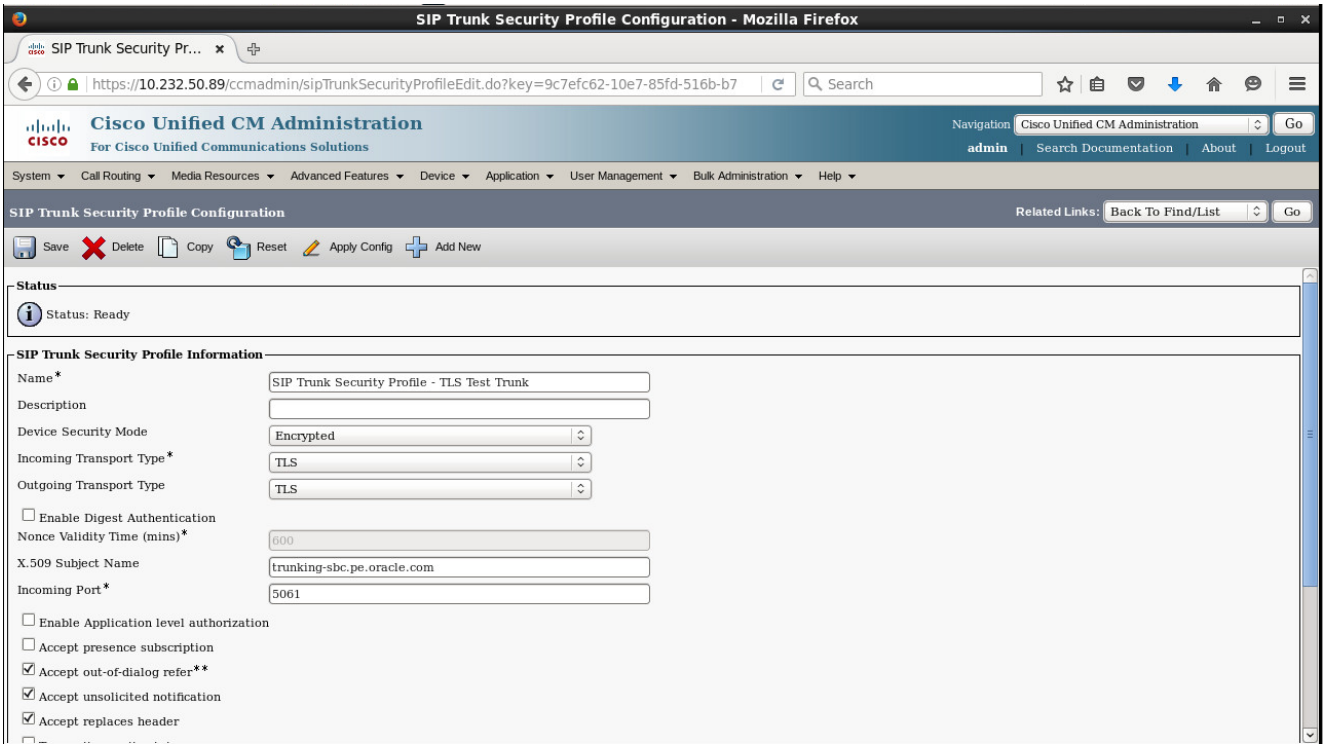
Click on Security, then SIP Trunk Security Profile.



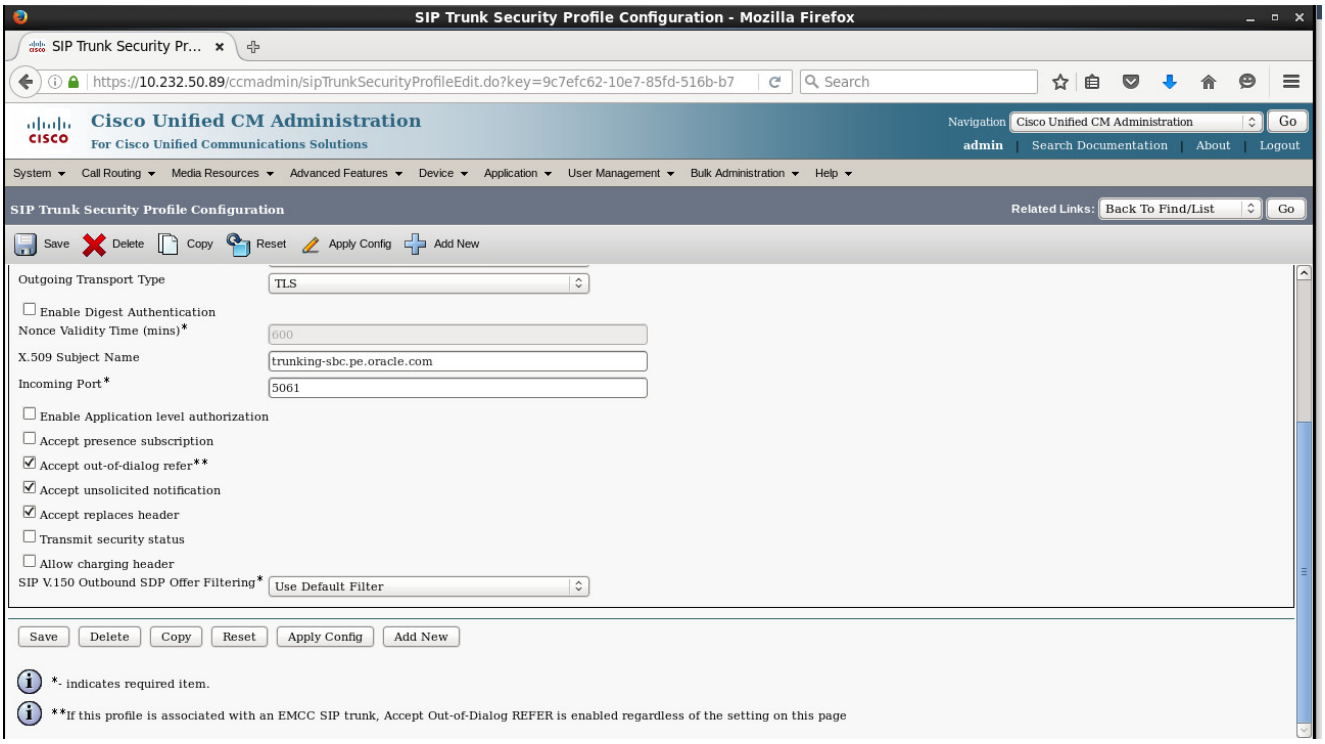
Click on Add New.



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.

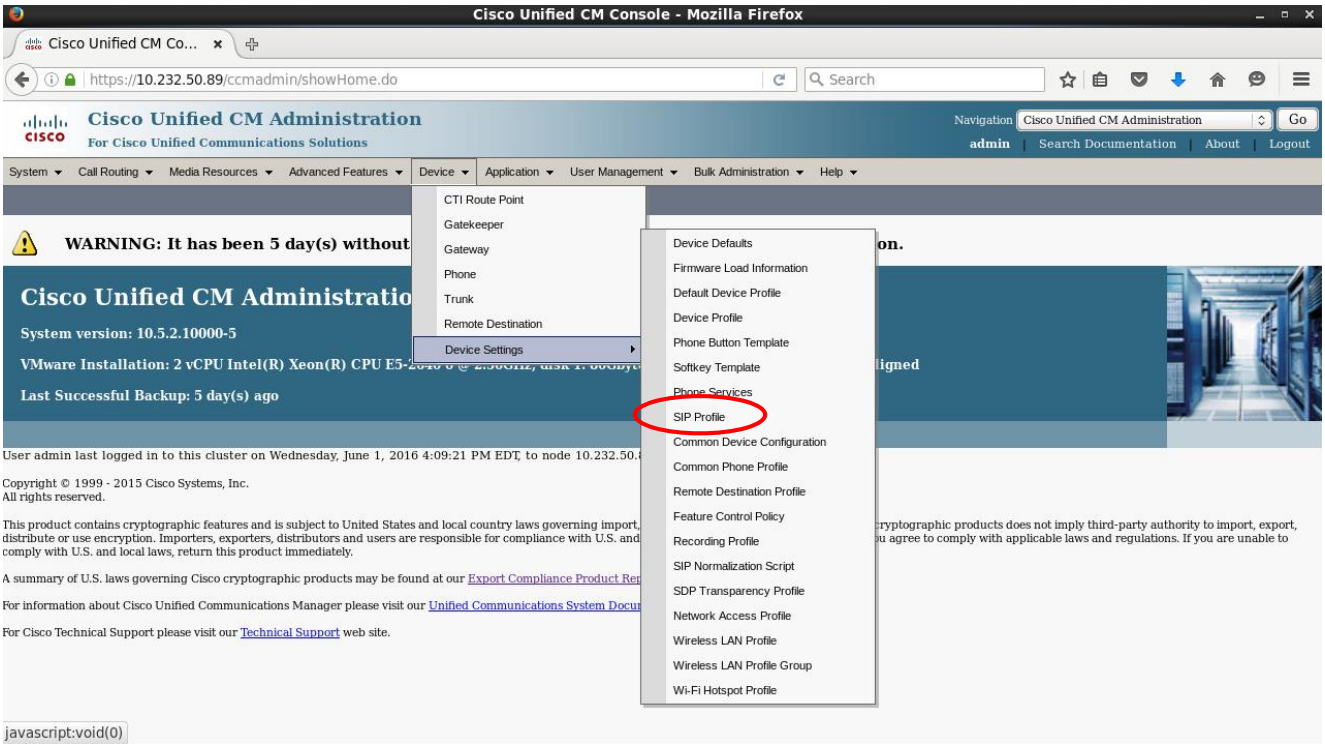


The remaining checkboxes should be selected as shown below. Then click Save.

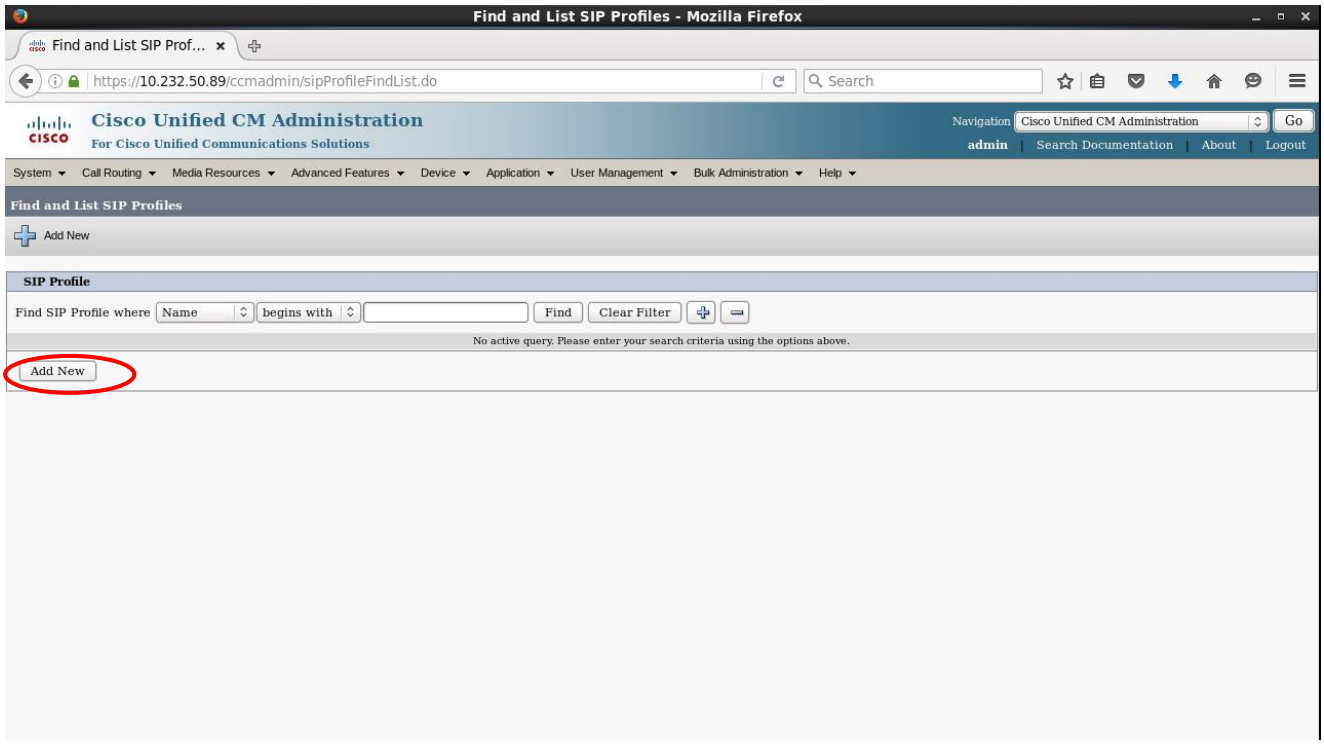


Creating a SIP Profile

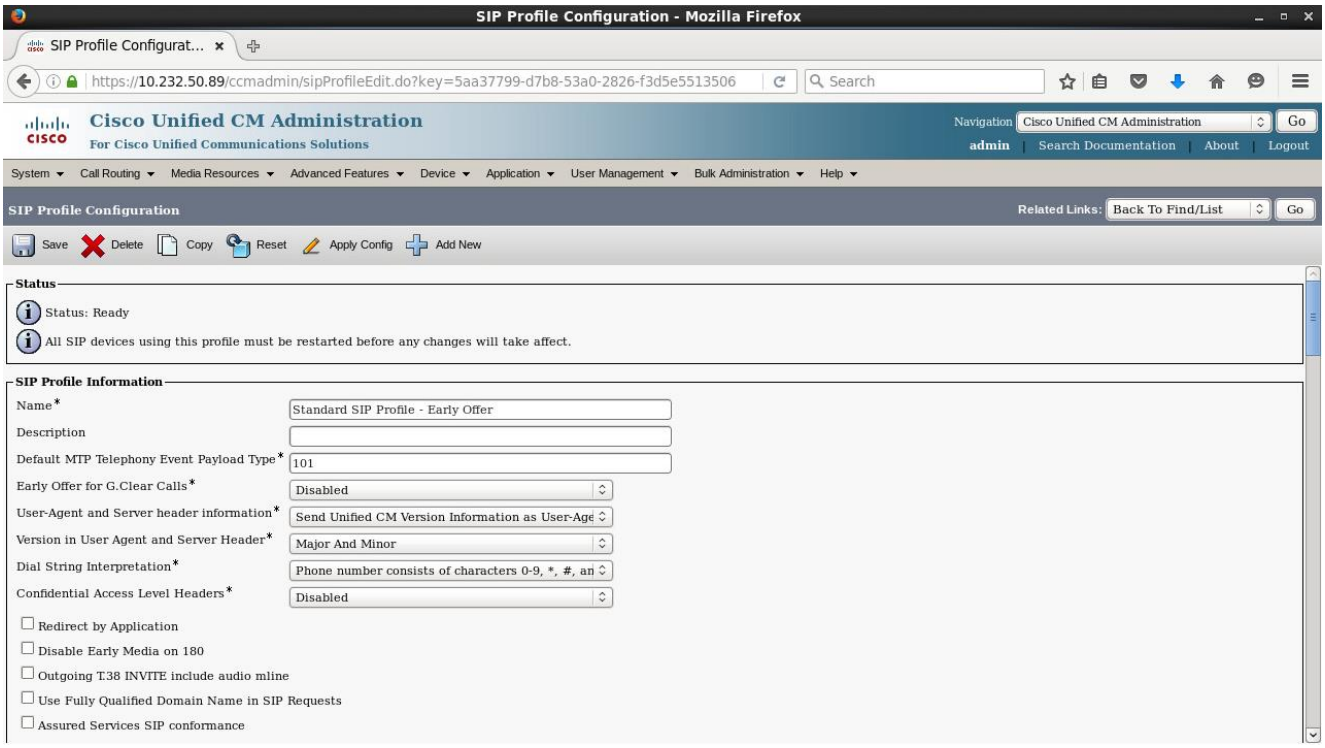
Click on Device, then Device Settings, then SIP Profile.



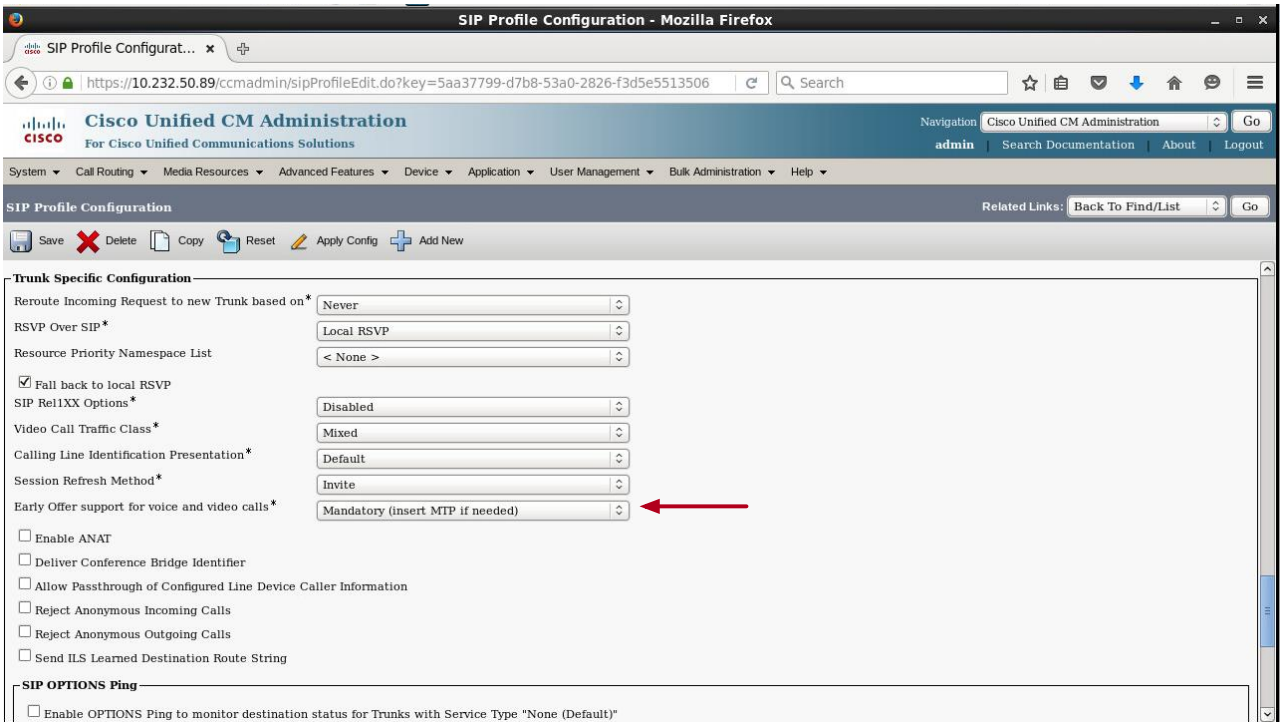
Click on Add New.



Use “Standard SIP Profile – Early Offer” as the Name.

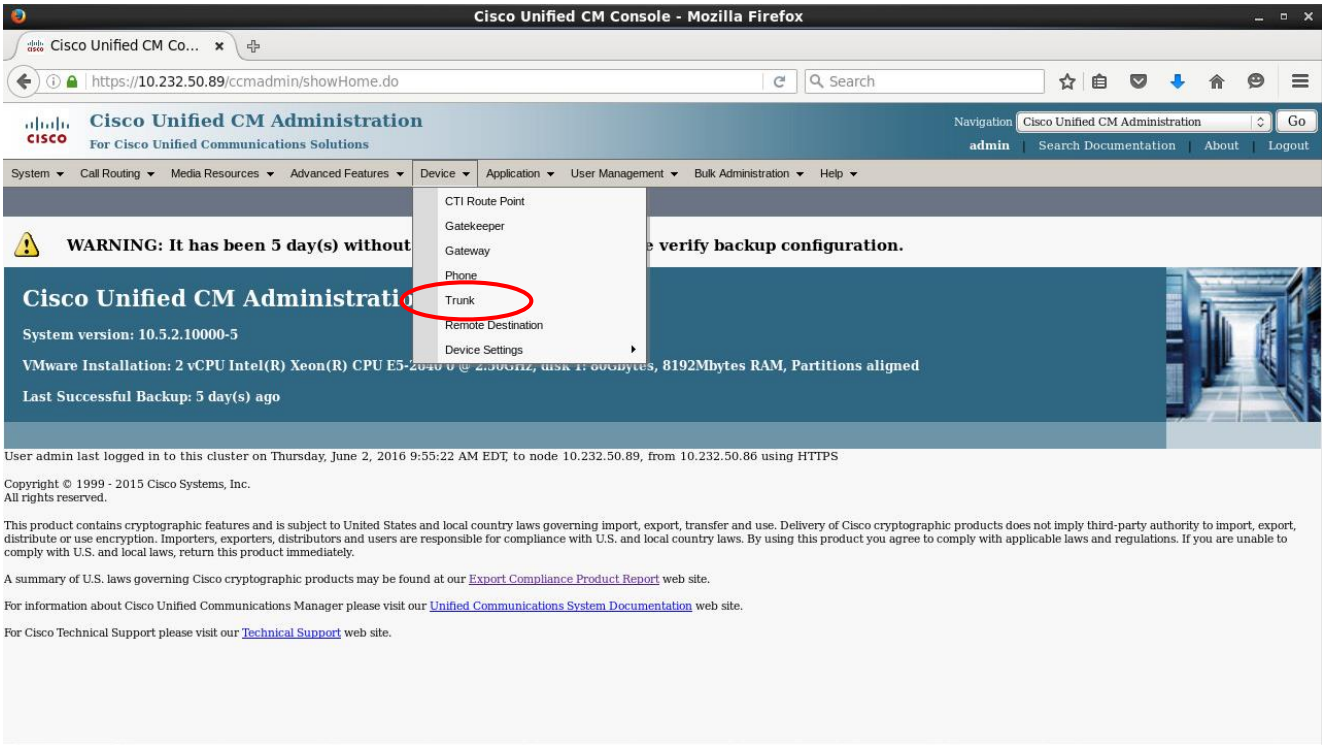


Scroll down to the Trunk Specific Configuration. Select “Mandatory (insert MTP if needed)” next to the Early Offer support for voice and video calls. Then click on Save.

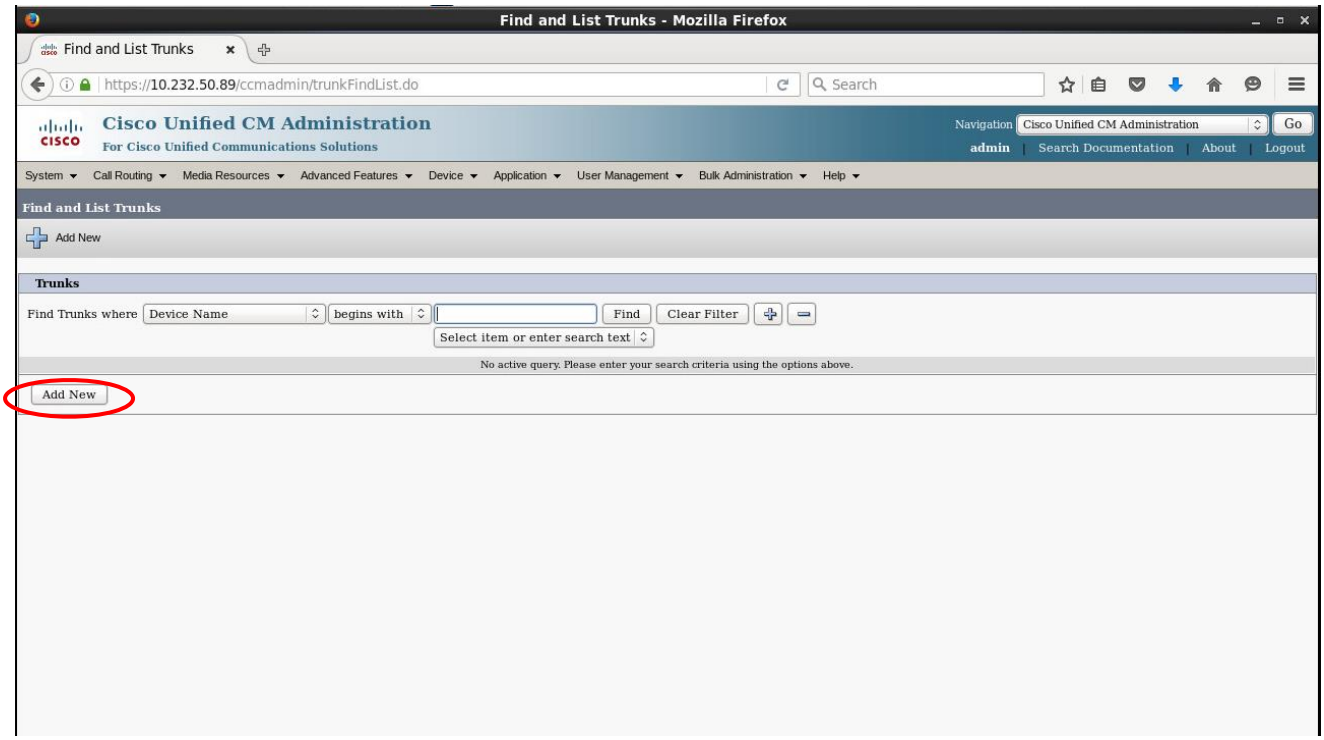


Configuring a SIP Trunk

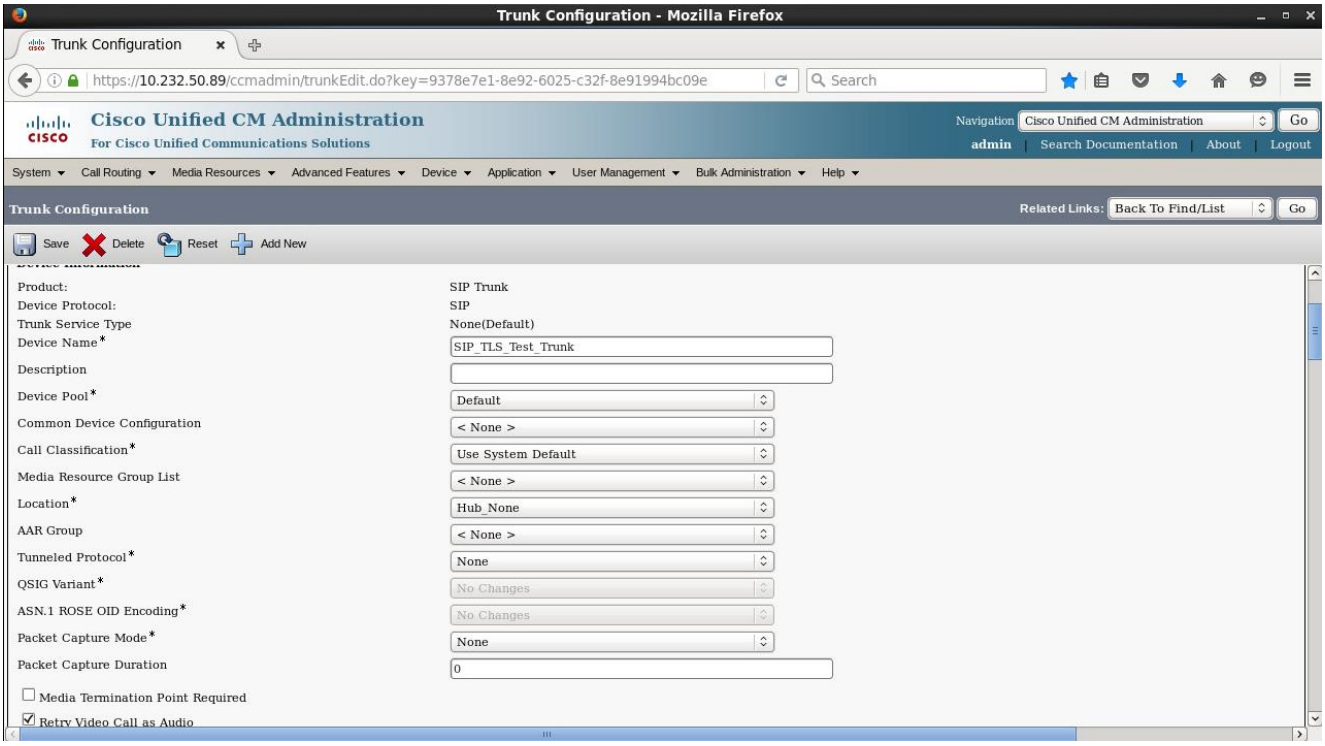
Click on Device, then Trunk.



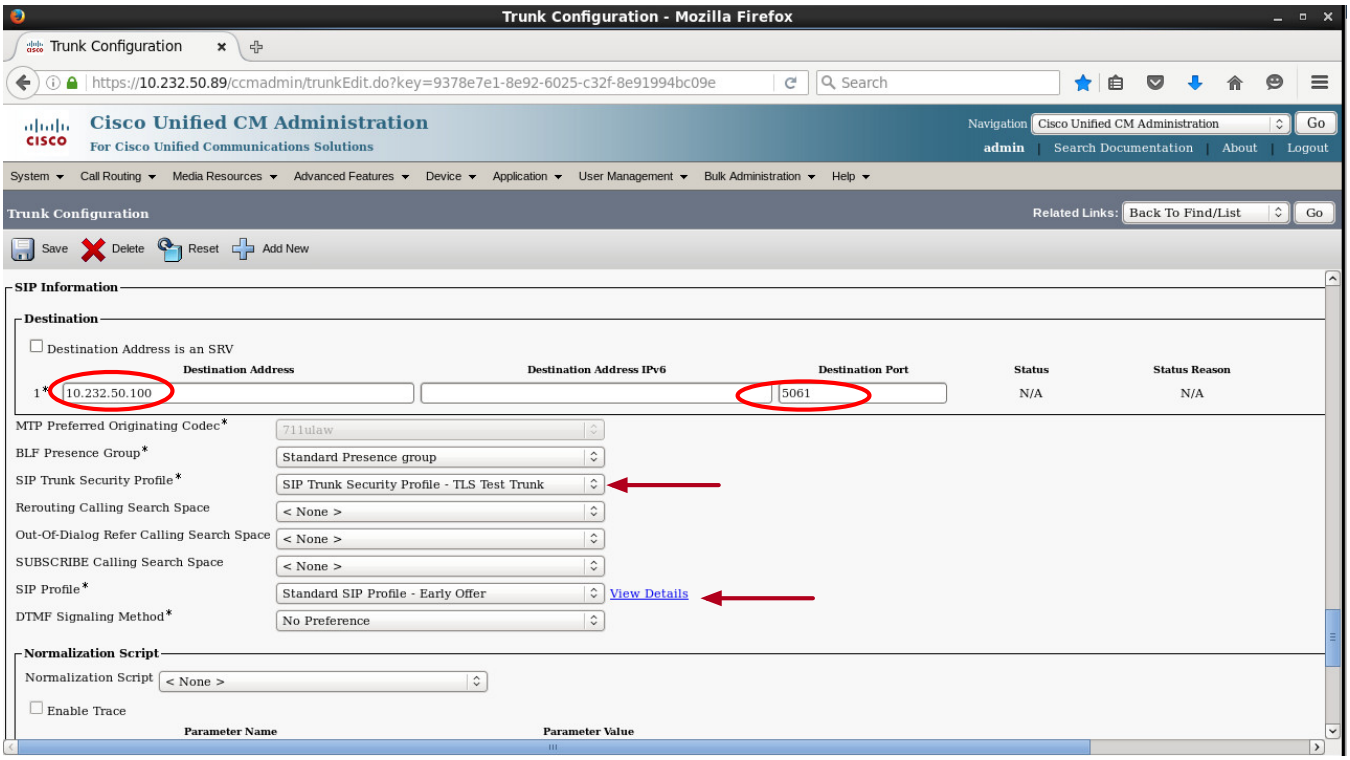
Click on Add New.



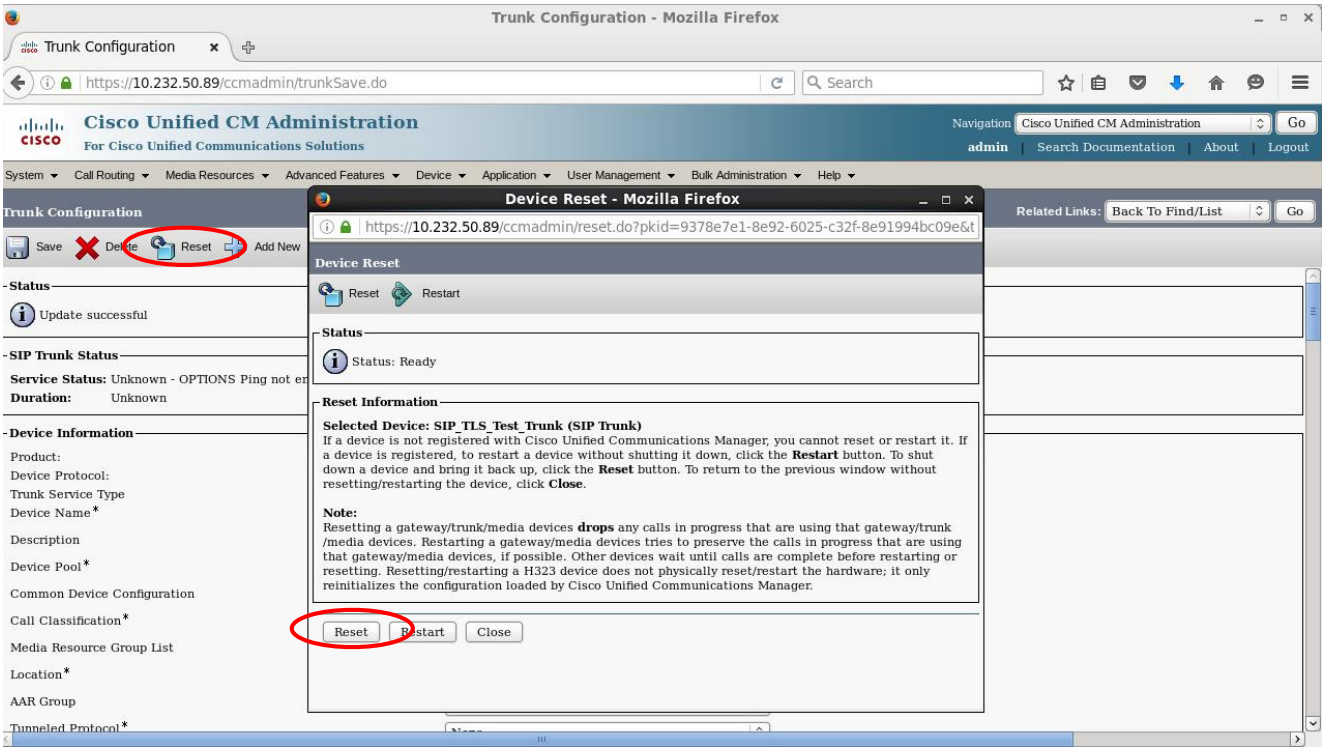
Give the trunk a name. SIP_TLS_Test_Trunk was used in this example. Set the other values shown below as appropriate for your CUCM installation.



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.

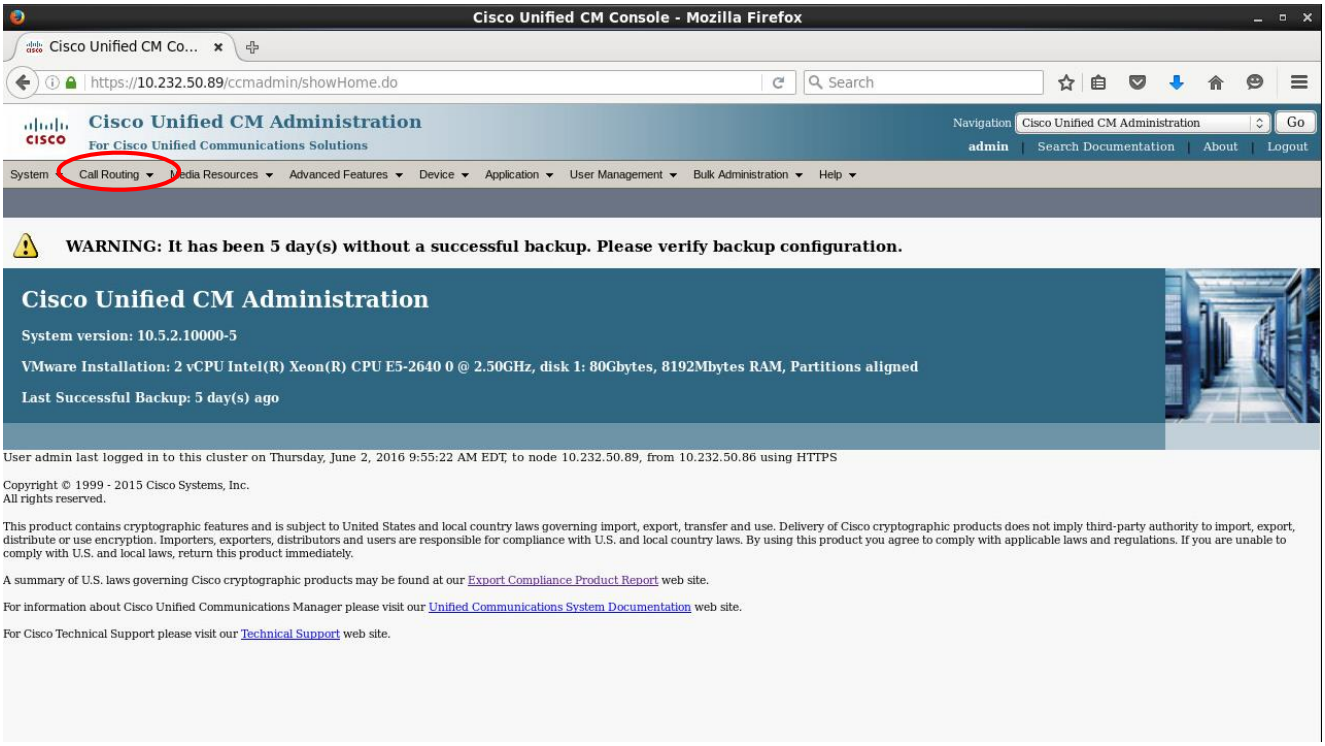


After saving, click on Reset, then click on Reset again in the pop up window.

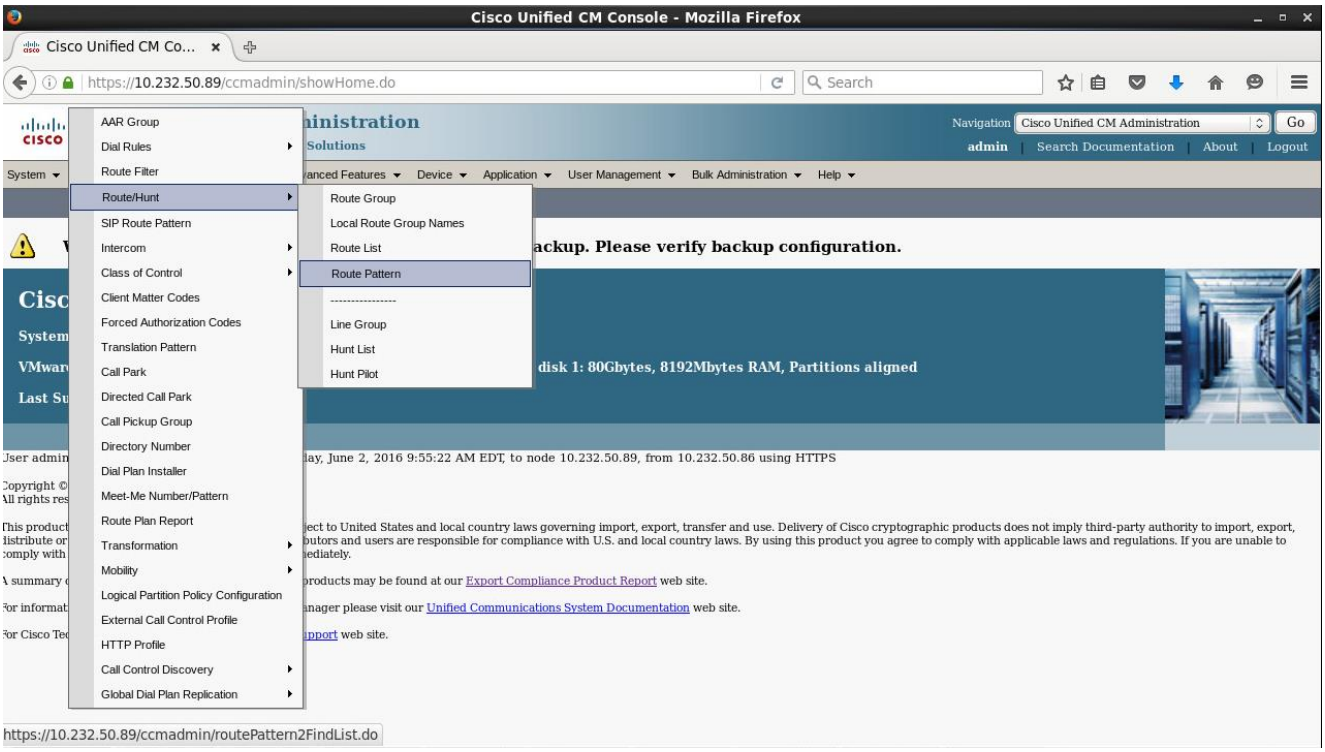


Creating a Route Pattern

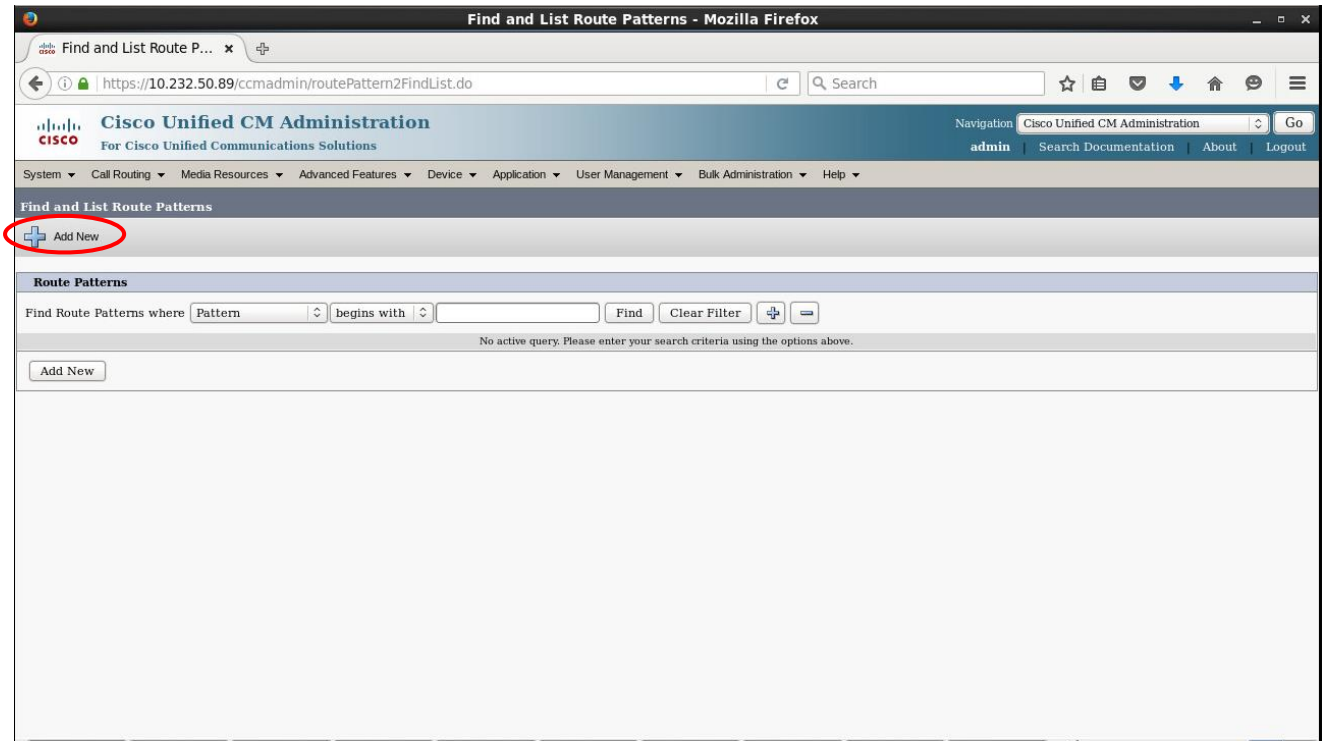
Click on Call Routing.



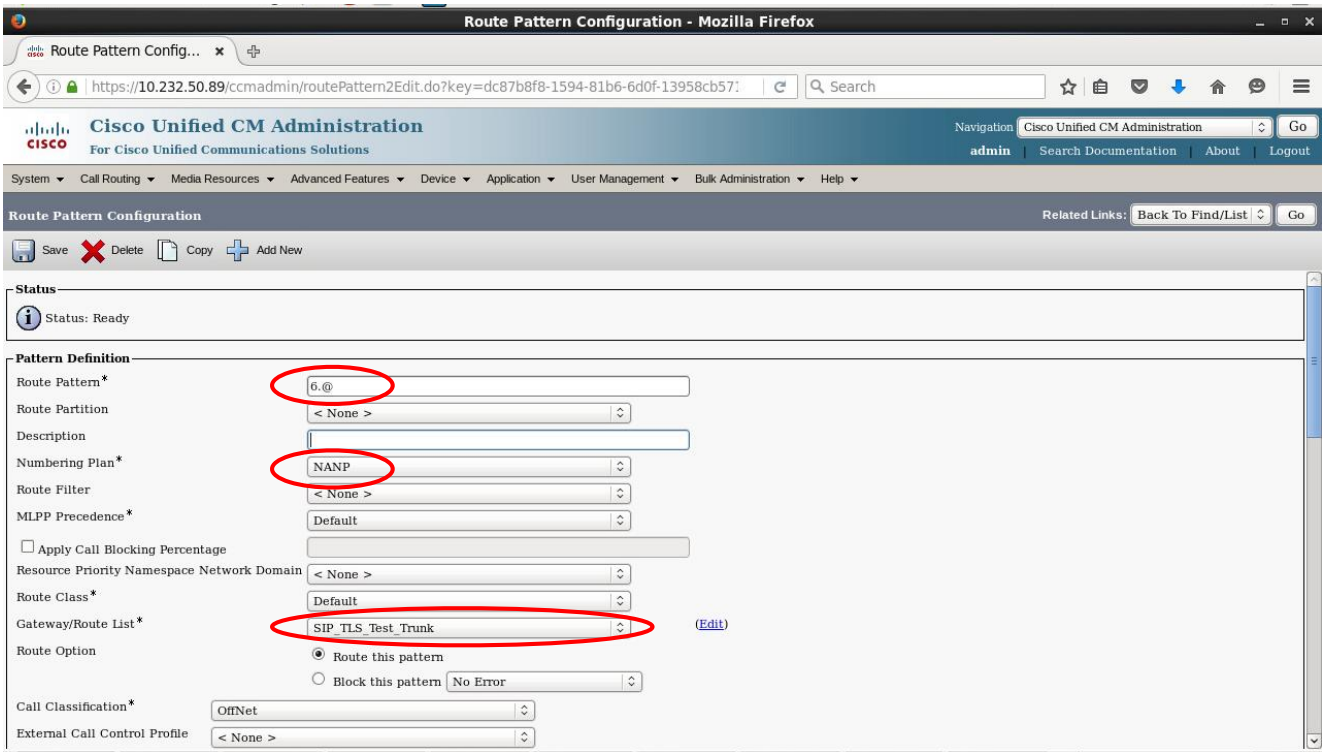
Click on Route/Hunt, then Route Pattern.



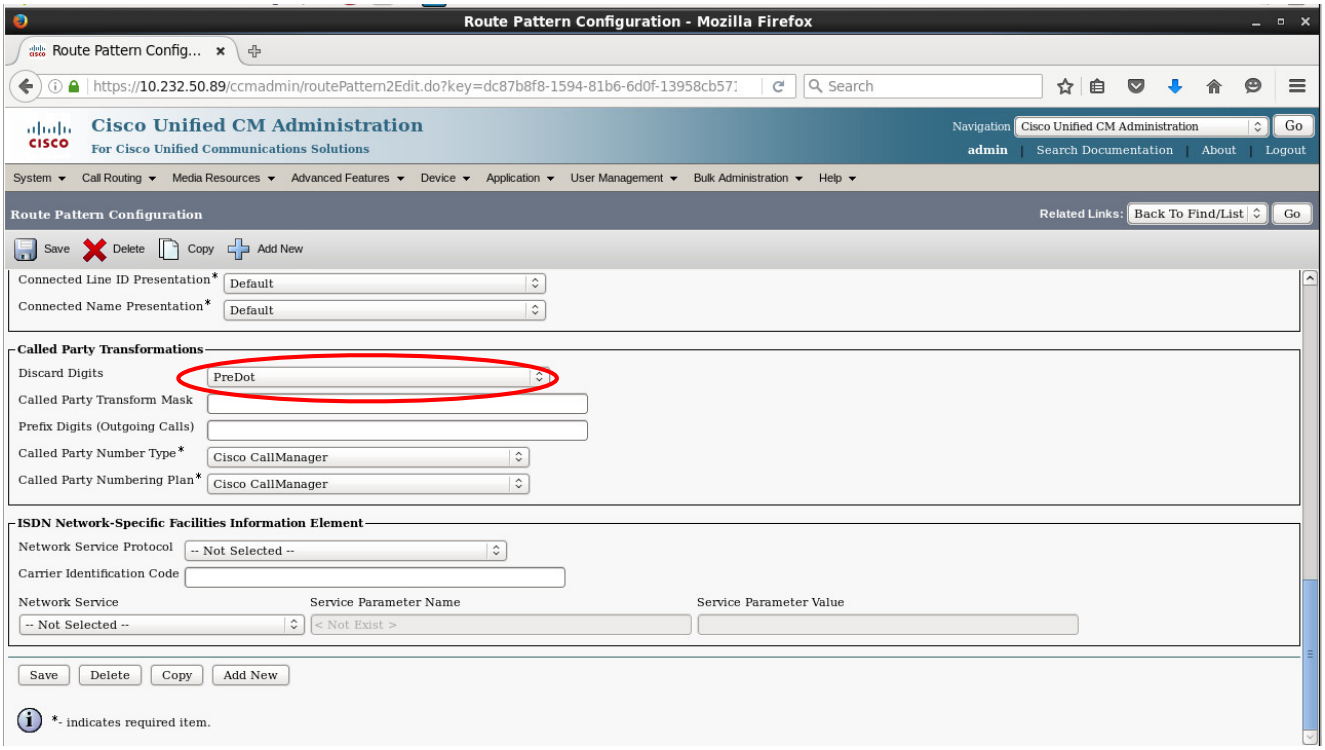
Click on Add New.



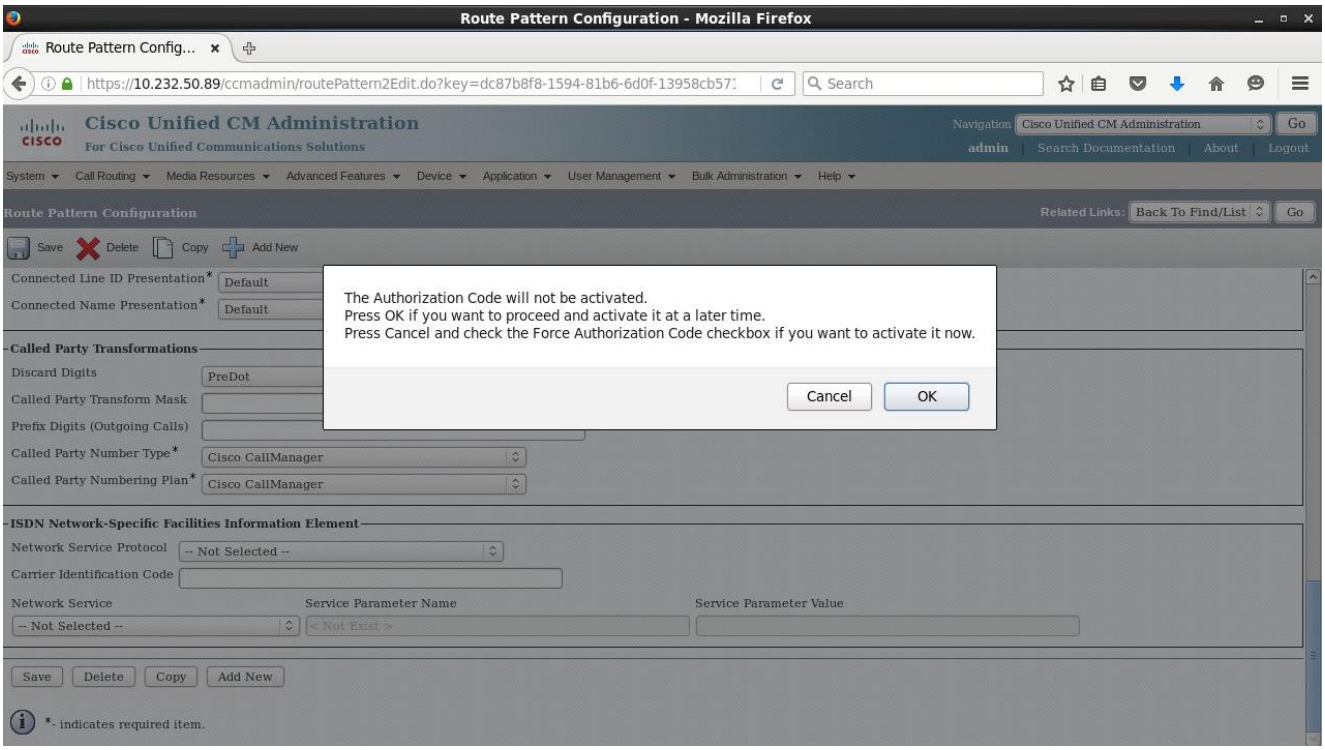
Enter an appropriate Route Pattern for your network. In this example, 6.@ was used which basically means that any number dialed beginning with 6 will route out the trunk. Select the Numbering Plan that is relevant to your network (NANP, or North American Numbering Plan, was used here). Select the previously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



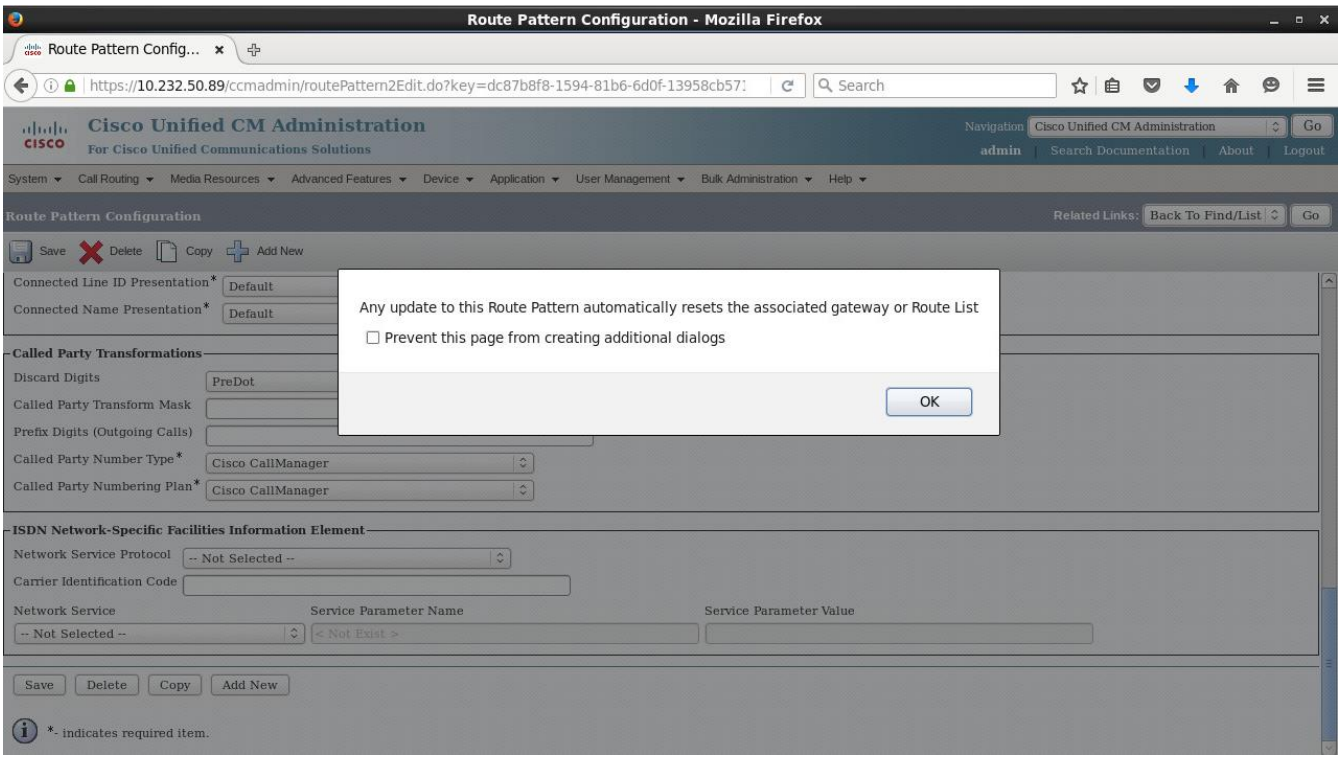
Scroll down to the Called Party Transformations. Select “PreDot” next to Discard Digits. This will discard the “6” in our example configuration. Then click on Save.



Click on OK in the pop up window.



Click OK again in the next pop up box.



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:

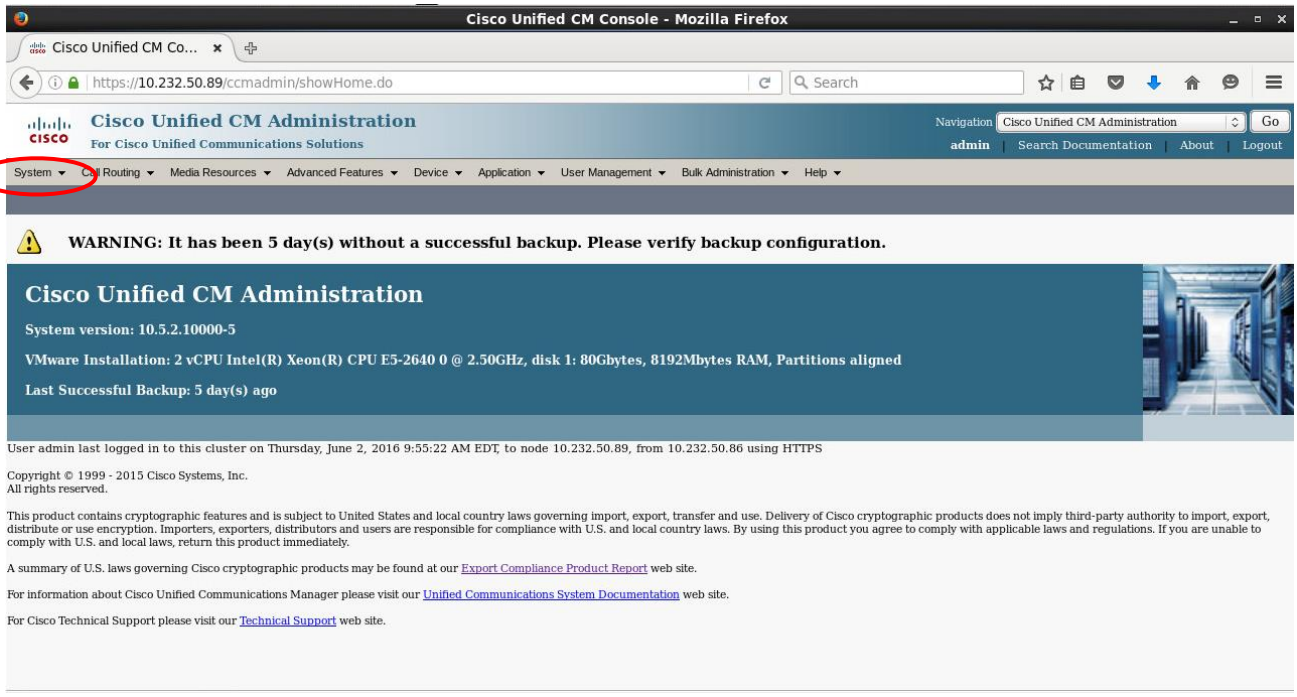
```
utils ctl set-cluster mixed-mode
```

Then issue the following command:

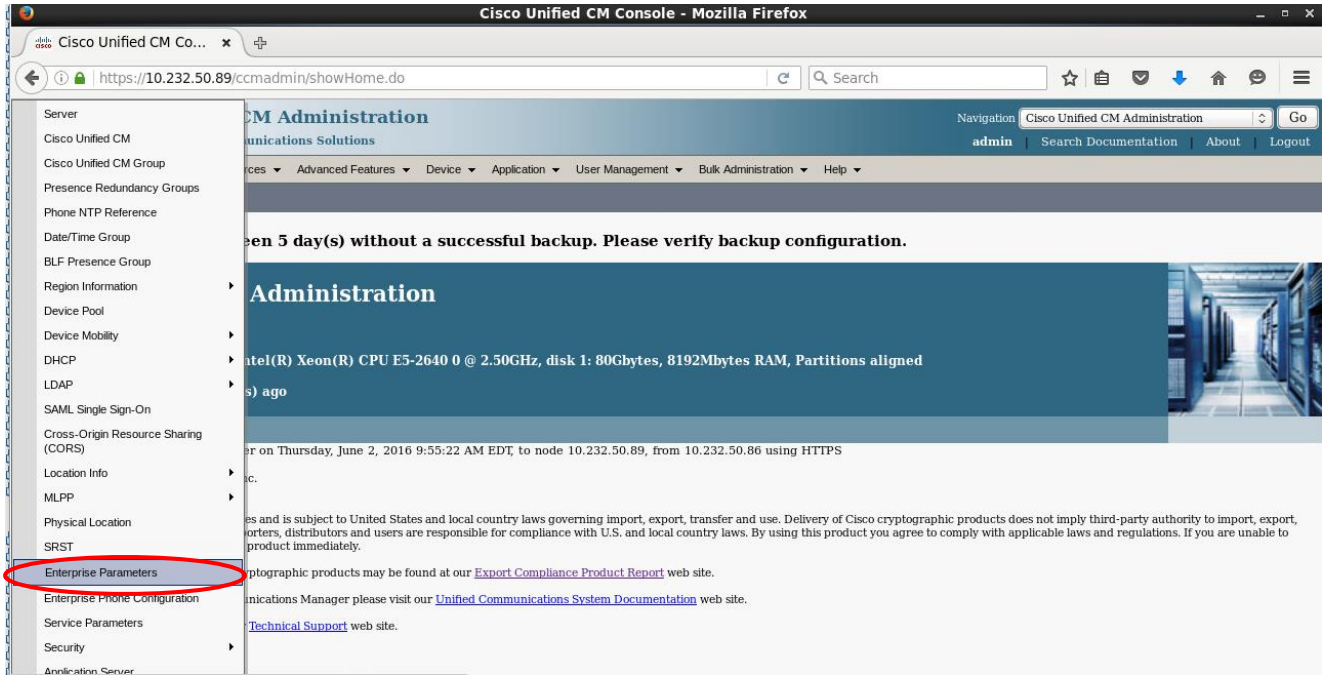
```
utils system restart
```

Then enter “yes” without the quotes. CUCM will reboot.

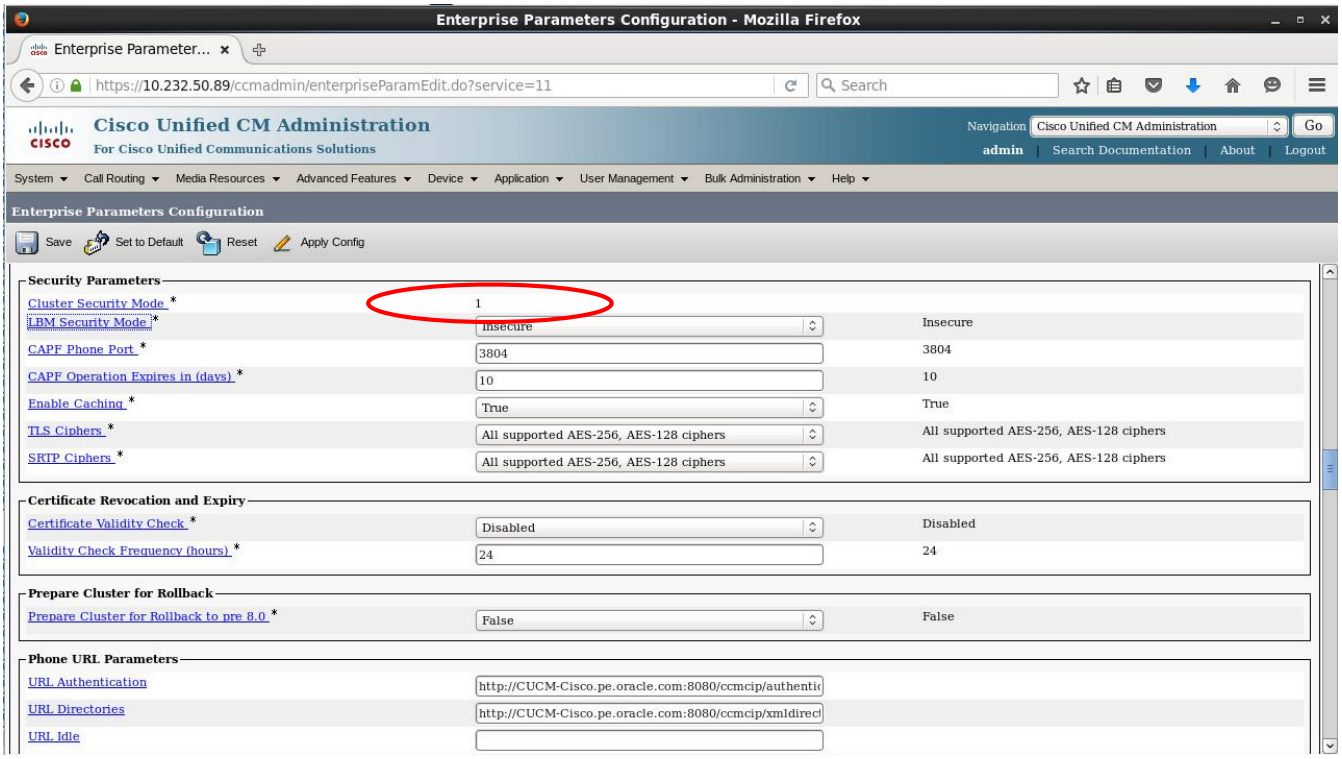
After the system reboots, login to CUCM’s web interface and click on System.



Select Enterprise Parameters.



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



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:

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

Examining the log files

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

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

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

Through the Web GUI

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

Oracle Enterprise Operations Monitor (EOM)

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

Appendix A

Accessing the ACLI

Access to the ACLI is provided by:

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

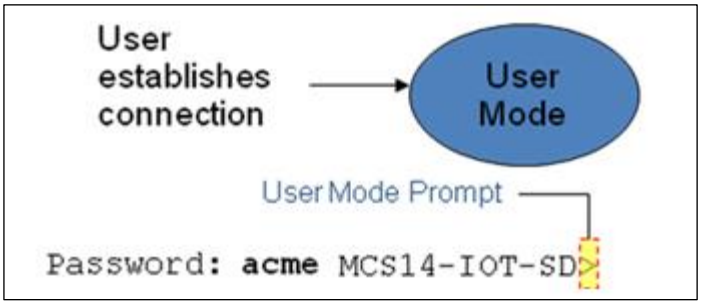
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

ACLI Basics

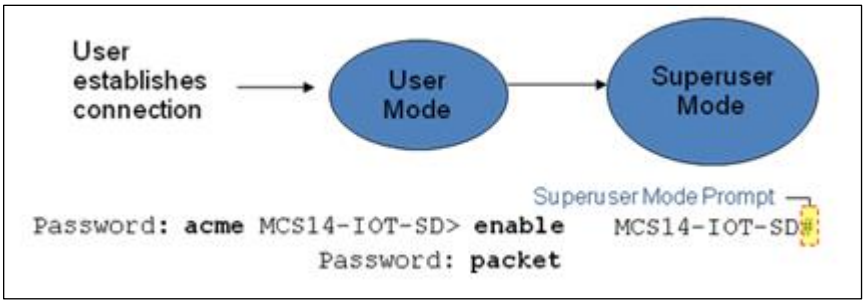
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

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

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



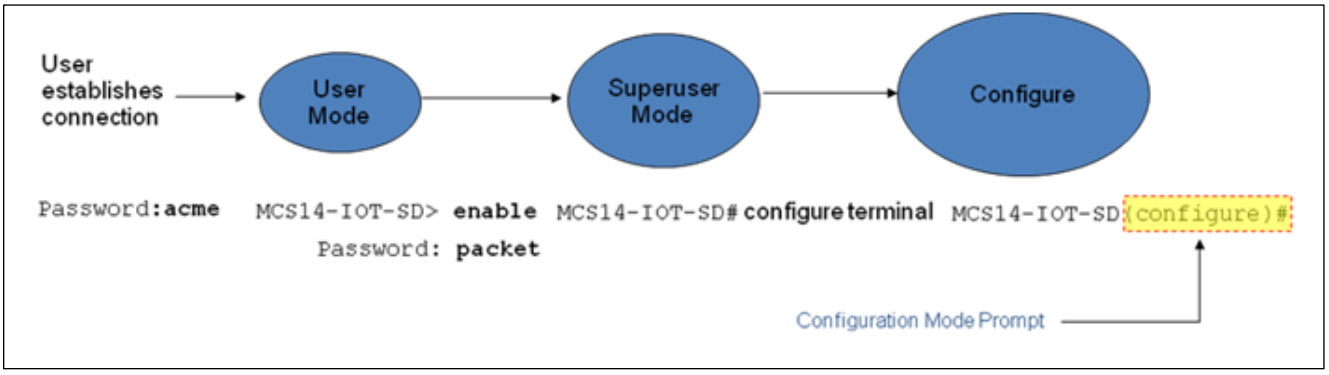
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



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

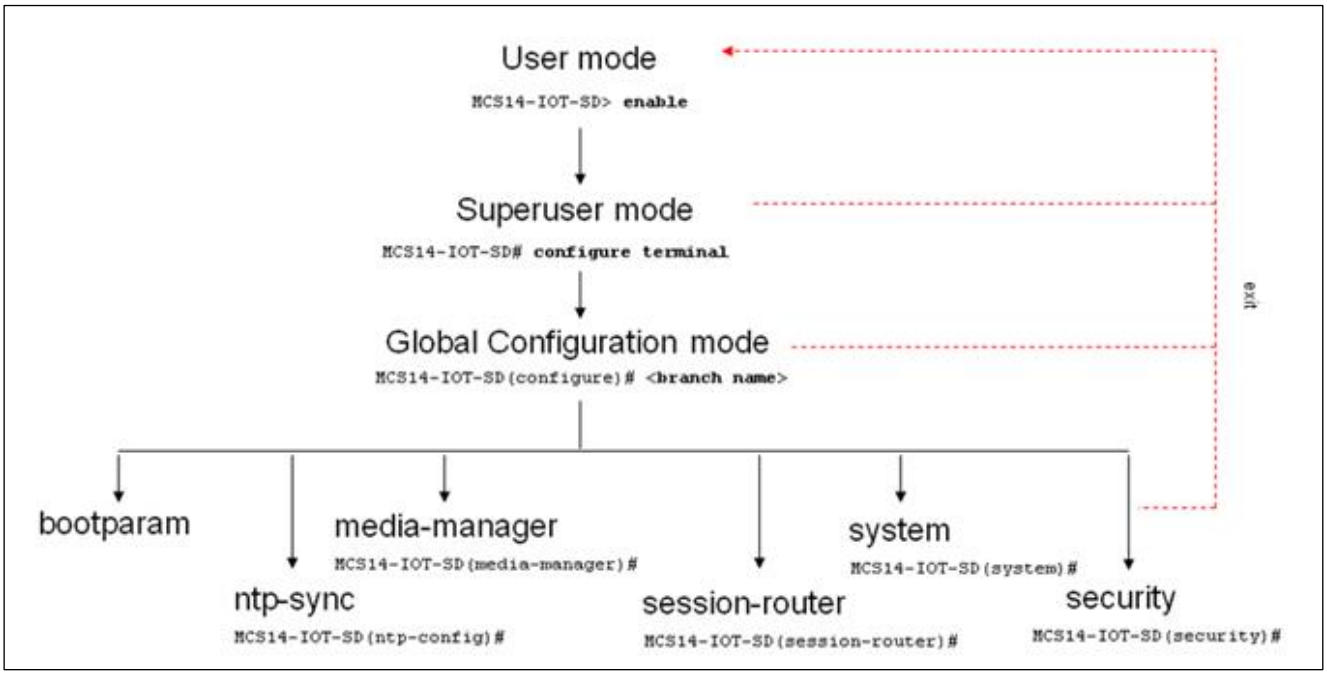
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the **`configure terminal`** command in the Superuser mode.

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



In the configuration mode, there are six configuration branches:

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



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

The bootparam branch provides access to SBC boot parameters.

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

The security branch provides access to security configuration.

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

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

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

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

Configuration Elements

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

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

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

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

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

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **`show`** command before issuing the **`done`** command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the **`done`** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the **`exit`** command to exit the selected element.

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

Editing an Element

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

1. Enter the element that you will edit at the correct level of the ACLI path.
2. Select the element that you will edit, and view it before editing it.
   The **`select`** command loads the element to the volatile memory for editing. The **`show`** command allows you to view the element to ensure that it is the right one that you want to edit.

3. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
4. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the **`show`** command before issuing the **`done`** command.
5. On completion, you must issue the **`done`** command.
6. Issue the **`exit`** command to exit the selected element.

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

Deleting an Element

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

To delete a single-instance element,

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

To delete a multiple-instance element,

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

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

Configuration Versions

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

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

Saving the Configuration

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

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

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

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

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

Activating the Configuration

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

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

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