TECHNICAL GUIDE to access Business Talk & BTIP Cisco CUCM and Webex Calling

versions addressed in this guide: CSR 15.0

Version of 28/10/2024

Table of contents

1 Goal of this document

The aim of this document is to list technical requirements to ensure the interoperability between Cisco CUCM IPBX with Business Talk IP SIP, hereafter so-called “service”.

2 Certified architectures

2.1 Introduction to architecture components and features

This document describes “only” the main supported architectures either strictly used by our customers or that are used as reference to add specific usages often required in enterprise context (specific ecosystems, redundancy, multi-codec and/or transcoding, recording…)

Concerning the fax support, Business talk and BTIP support the following usage:

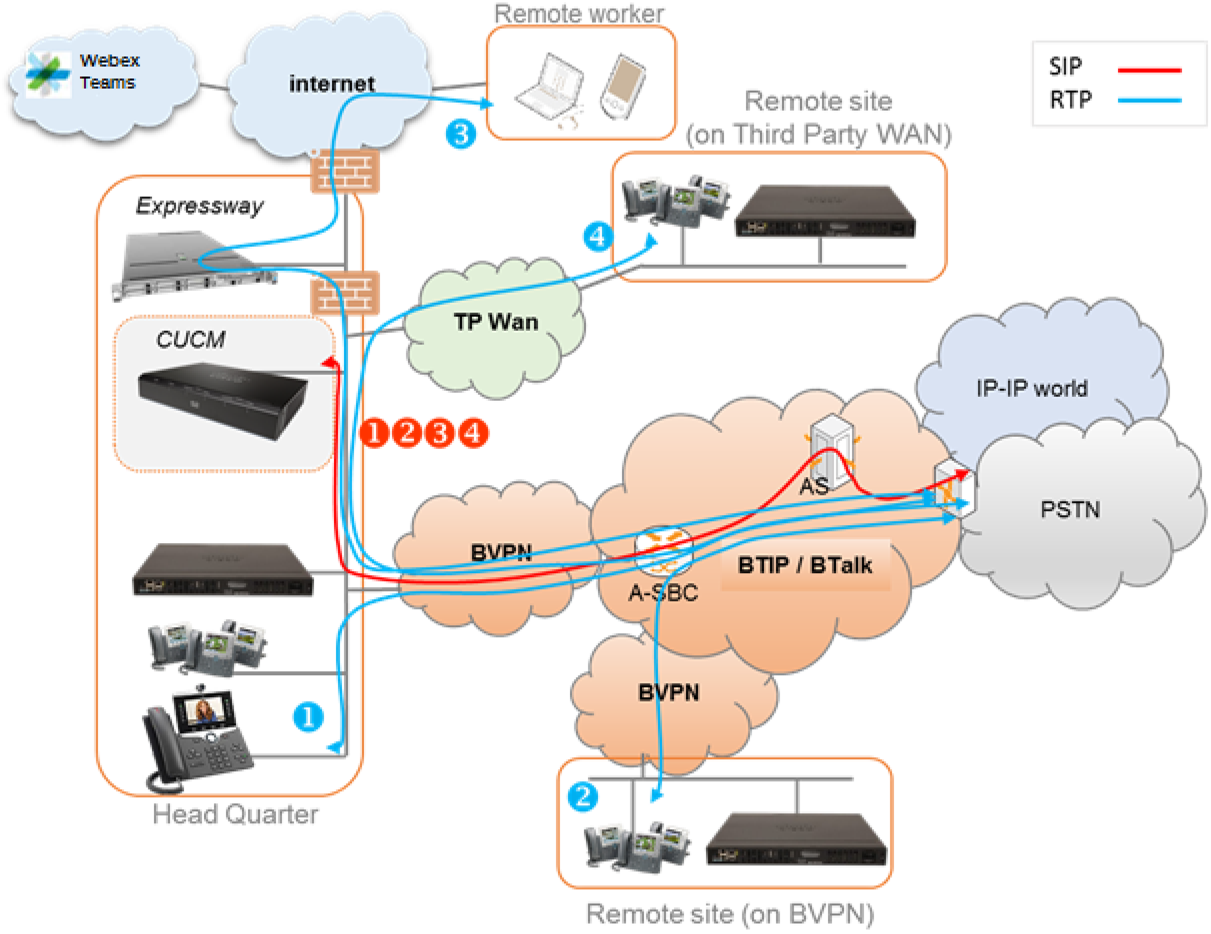
- fax servers connected to the IPBX -and sharing same dial plan-, or as separate ecosystems -and separate dial plan-
- analog fax machines, usually connected on specific gateways* (seen as IPBX ecosystem or not)

Fax flows are handled via T.38 transport only.

Concerning the Quality of Service, Business VPN and BTIP/BTalk networks trust the DSCP (Differenciated Services Code Point) values sent by customer voice equipment. That’s why Orange strongly recommends to set the IPBX, IP phones and other voice applications with a DiffServ/TOS value = 46 (or PHB value = EF) at least for media.

‘BTIP DROM’ architectures are now supported. Dedicated aSBC pairs have been installed in Caribbean and Indian Ocean zones for local calls. For a trunking point of view, the mechanism is like ‘BTIP out of France’, the IPBX must support international dial plans and route local calls to the dedicated aSBC pair.

2.2 CUCM without CUBE



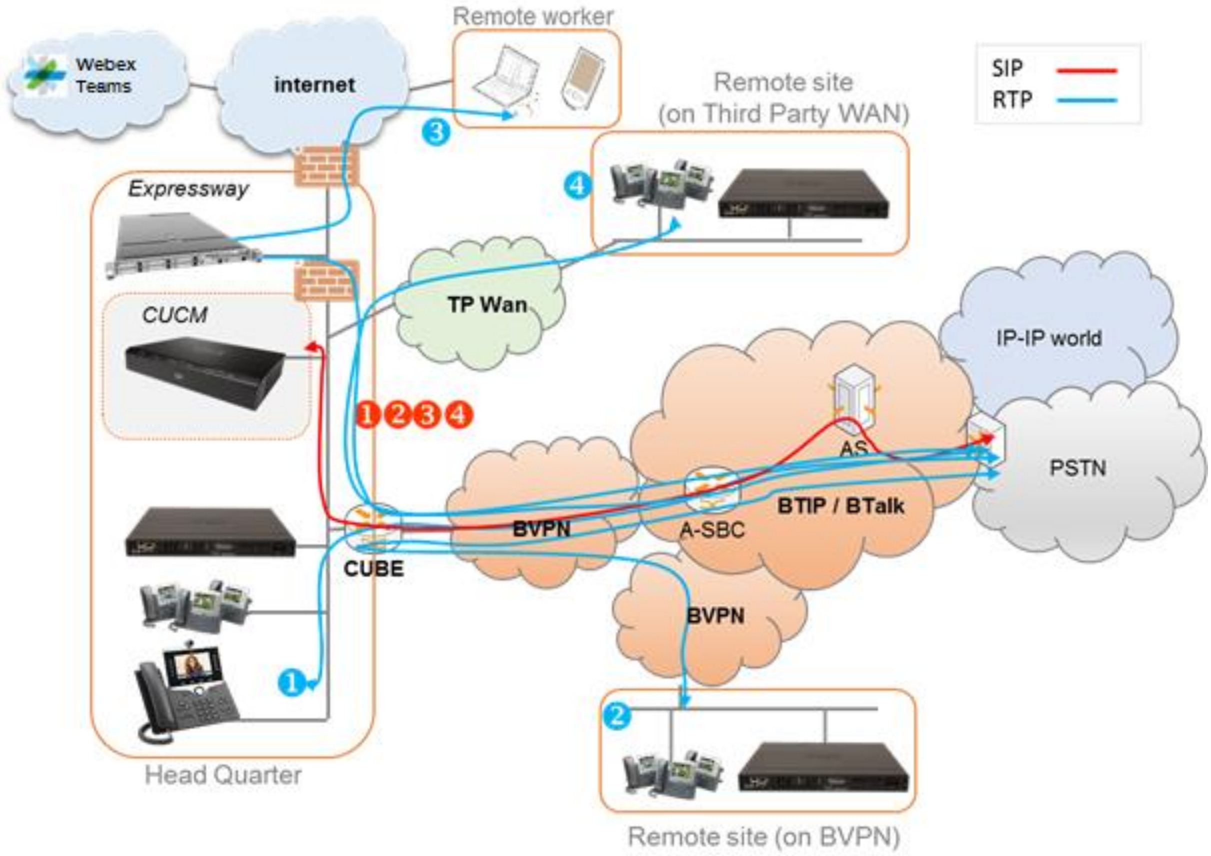
Notes :

- in the diagram above, the SIP, proprietary and Webex Teams internal flows are hidden.
- call flows will be the similar with or without CUCM redundancy

In this architecture :

- all 'SIP trunking' signaling flows are carried by the CUCM server and routed on the main BVPN connection.
- Media flows are direct between endpoints and the Business Talk/BTIP but IP routing differs from one site to another :
  - For the Head Quarter site, media flows are just routed on the main BVPN connection
  - For Remote sites on BVPN, media flows are just routed on the local BVPN connection (= **distributed architecture**),
  - For Remote sites on Third Party WAN, media flows are routed through the Head Quarter (but not through the IPBX) and use the main BVPN connection (= **centralized architecture**).

2.3 CUCM with CUBE



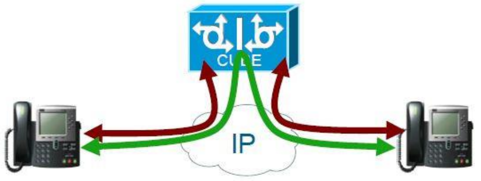
Notes :

- in the diagram above, the SIP, proprietary and Webex Teams internal flows are hidden.
- call flows will be similar with or without CUCM redundancy.

In this architecture, all SIP trunks are anchored by the CUBE but with 2 modes for the media :

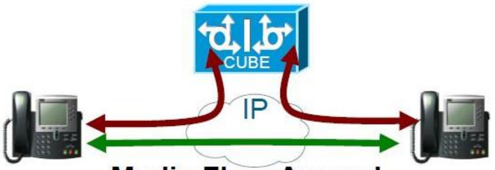
- “Flow-through” mode → signalling and media flows cross the CUBE.
- “Flow-around” mode → signaling flows cross the CUBE, but media flows go directly towards endpoints

Note: BToI/BTIPoI only work with flow-through mode due to transcoding between RTP and SRTP performed on CUBE.



Media Flow-Through

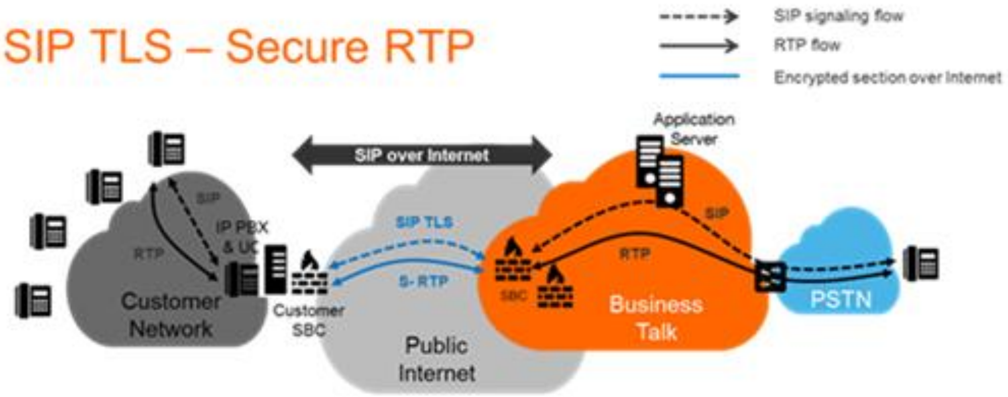
- Signaling and media terminated by the Cisco Unified Border Element
- Transcoding and complete IP address hiding require this model



Media Flow-Around

- Only Signaling is terminated on CUBE
- Media bypasses the Cisco Unified Border Element

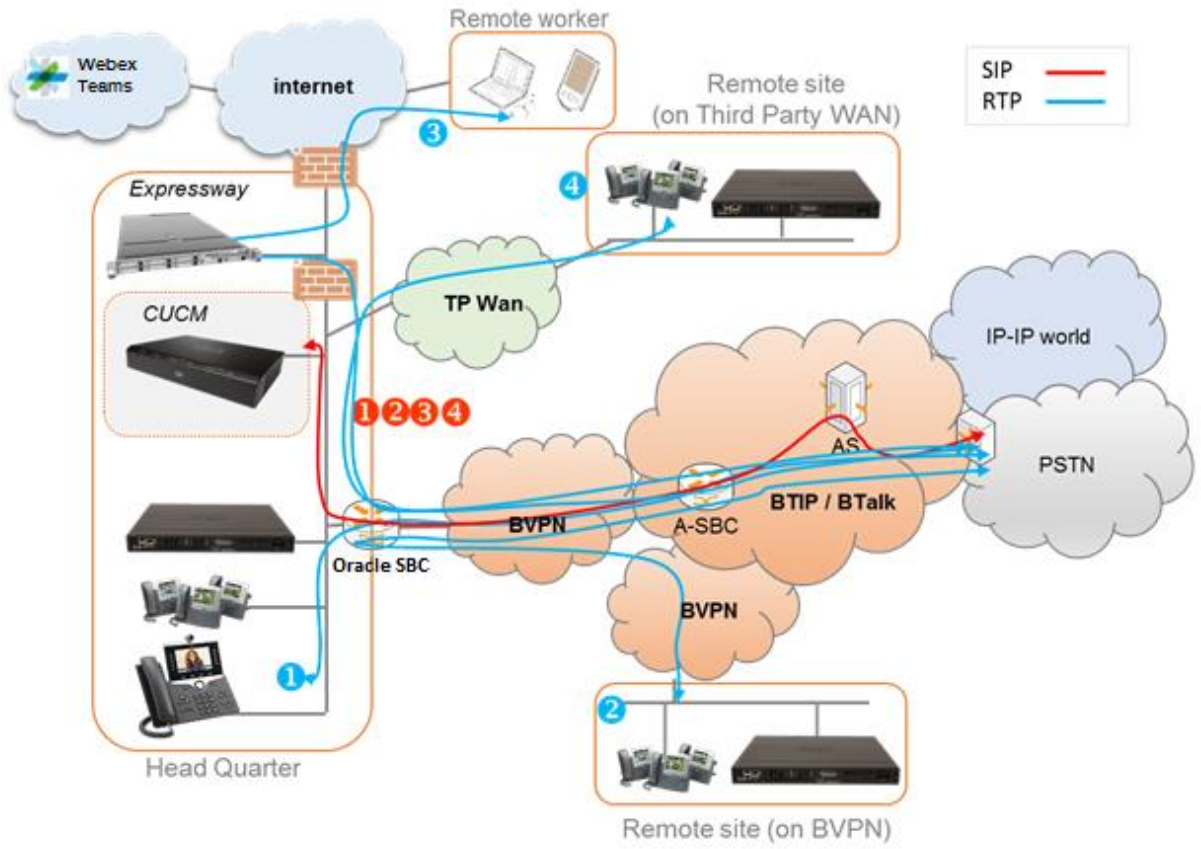
2.3.1 Business Talk over Internet (BToI) & Business Talk IP over Internet (BTIPoI)



In this architecture, all SIP trunks are anchored by the CUBE in flow-through mode for the media. Traffic between CUBE and Orange A-SBC is carried over public internet. The traffic is encrypted with TLS v.1.2 for signalization and SRTP for media. CUBE on ISR G3 chassis performs transcoding between RTP and SRTP by default therefore internal traffic within customer site can be unencrypted.

BToI/BTIPoI architecture has been certified with CUCM 12.5/14.0 and CUBE ISR 4000 series running IOS-XE 16.9.5 & 17.3.2 & 17.3.4.

2.4 CUCM with Oracle SBC



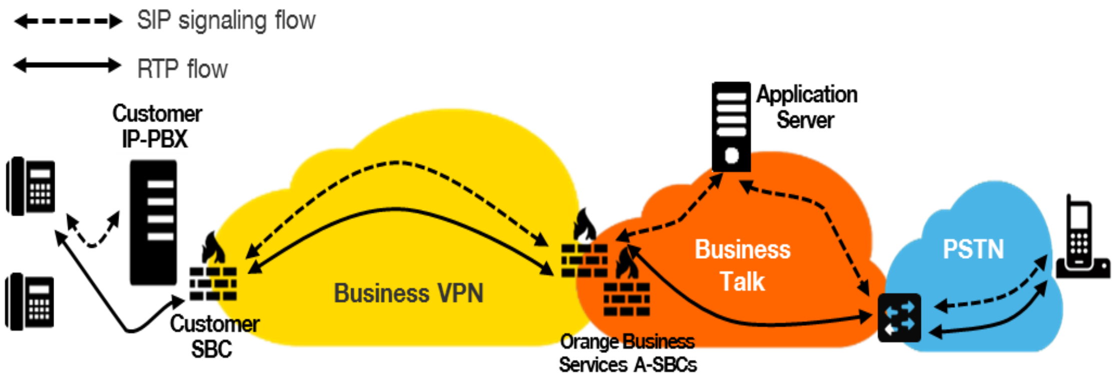
In this architecture, all SIP trunks are anchored by the Oracle Enterprise SBC. The call flows are very similar to the architecture with Cisco CUBE. Session Border Controller is mostly transparent for SIP traffic. It can also be used for TLS encryption ensuring secure traffic between Oracle ESBC and Orange SBC.

Oracle Enterprise SBC v.8.2 has been validated with Cisco CUCM v.12.0.

The following features have been tested for CUCM with Oracle SBC integration:

- Basic Telephony features (basic calls, CLIR, forward, transfer, MoH, DTMF)
  - IP Phones
  - FXS Gateway for analog phones
- Fax
  - Sagem Xmedius Fax server
  - SIP Fax on FXS Gateway
- TLS Encryption between Oracle ESBC and Orange SBC

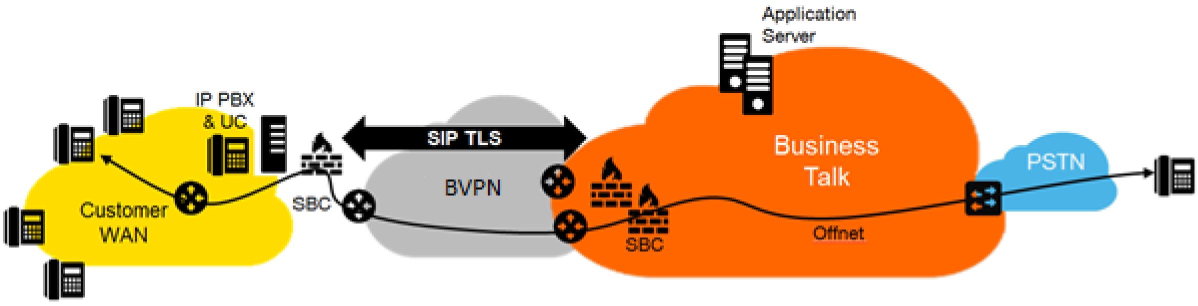
2.4.1 Unsecured SIP Trunk



In this architecture :

- Both ‘SIP trunking’ and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the “customer SBC”. For the Head Quarter & remote sites sites, media flows are routed through the SBC and the main BVPN connection.
- Both ‘SIP trunking’ on North (OBS Carrier) and South side of the SBC must be configured in “clear” mode though UDP.

2.4.2 Secured SIP Trunk



In this architecture :

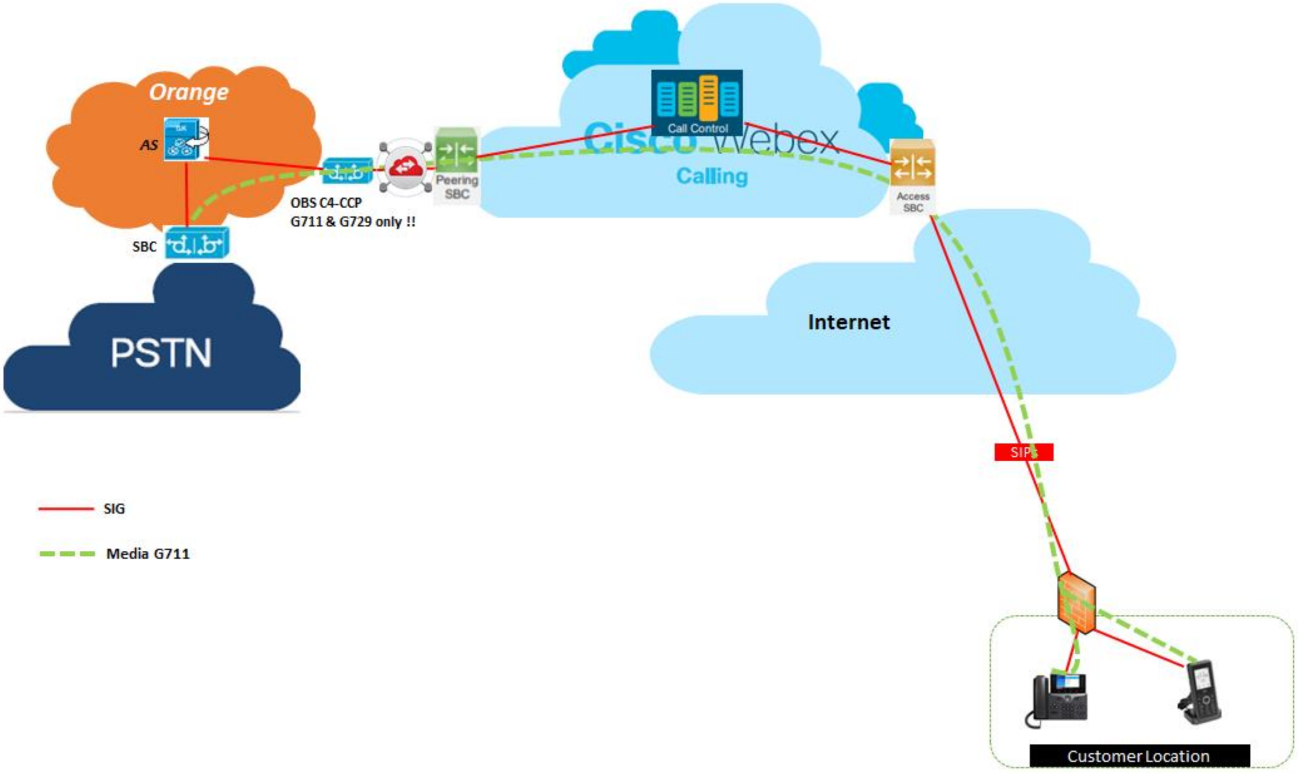
- both ‘SIP trunking’ and RTP media flows between endpoints and the Business Talk/BTIP are anchored by the “customer SBC”. For the Head Quarter & remote sites sites, media flows are routed through the SBC then BVPN.
- ‘SIP trunking’ on North (OBS Carrier) side of the SBC must be configured in “secured” mode through TLS encryption and media SRTP encryption.

2.5 Webex Calling MT & DI

2.5.1 Webex Calling MT - Webex Workplace Together

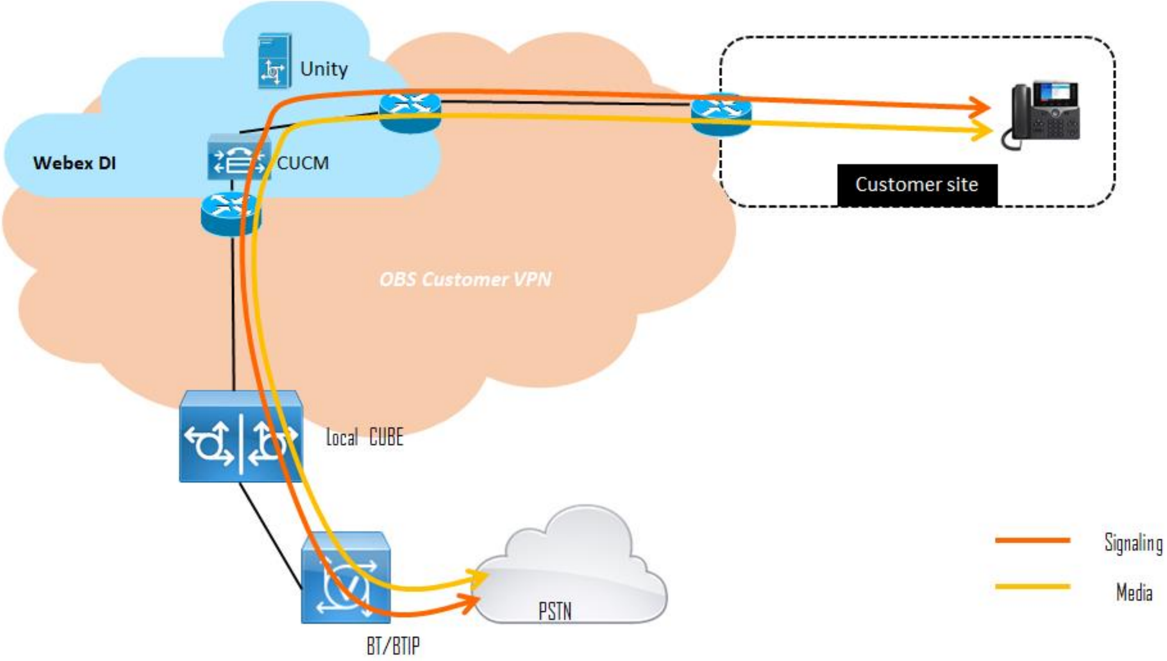
NOTE: Webex Calling Multi-Tenant is sold by Orange Business only as 'Workplace Together Webex' offer.

A direct "class 4" operator trunk is set up between Orange and Cisco infrastructure. No additional equipment is necessary.



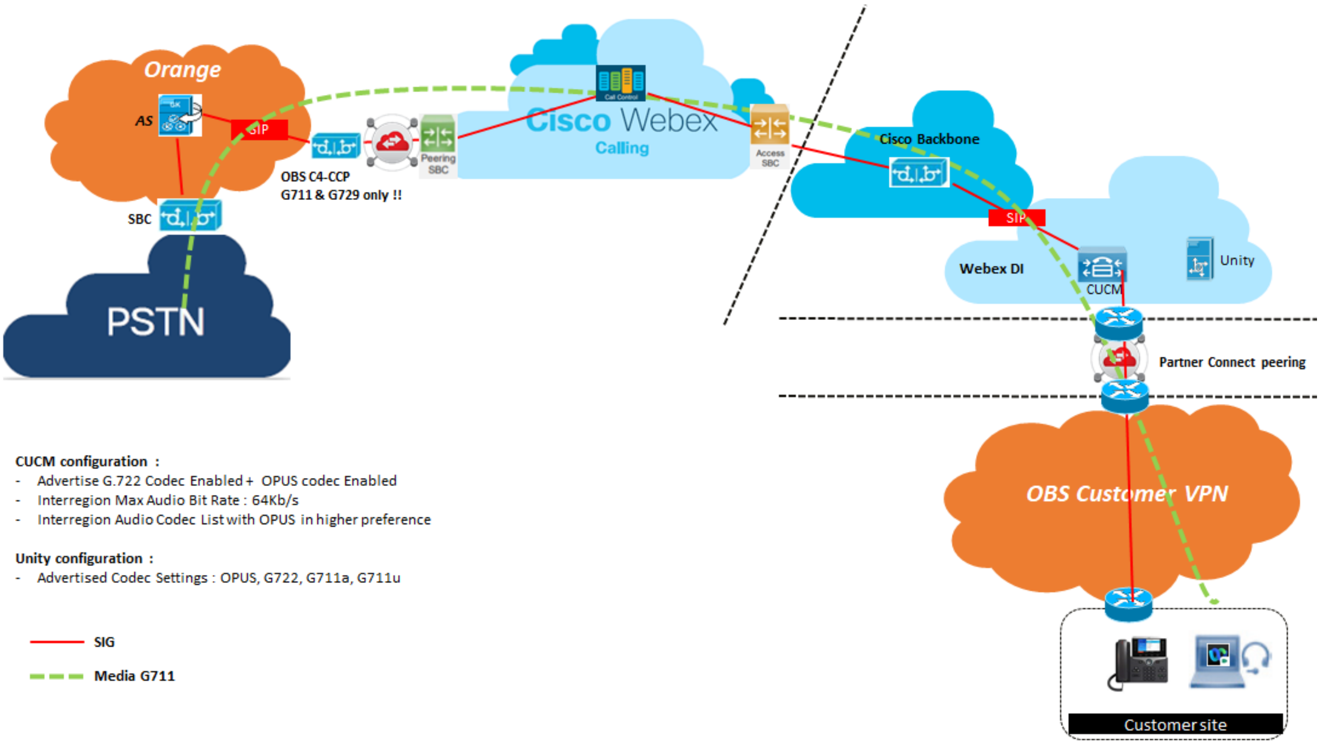
2.5.2 Webex Dedicated Instance – Local CUBE connection

This architecture uses Webex DI with local CUBE deployed on customer site connected via VPN. All supported access options are available between CUBE and Orange access SBC (through Orange BVPN or BTIP/BTalk over Internetl). It is possible to set up this connection without the use of CUBE, however such architecture should be analyzed on demand.



2.5.3 Webex Dedicated Instance – Multitenant connection

This architecture uses interconnection through Cisco backbone infrastructure between Webex DI and Webex Calling MT. Business Talk infrastructure is then reached through Webex Calling as described in sections 2.5.1.



CUCM configuration :

- Advertise G.722 Codec Enabled + OPUS codec Enabled
- Interregion Max Audio Bit Rate : 64Kb/s
- Interregion Audio Codec List with OPUS in higher preference

Unity configuration :

- Advertised Codec Settings : OPUS, G722, G711a, G711u

3 Parameters to be provided by customer to access service

IP addresses marked in red have to be indicated by the customer, depending on customer architecture scenario.

3.1 CUCM without CUBE

Head Quarter (HQ) or Branch Office (BO) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
CUCM Business Edition (1 server)	No reduncdancy (1 Publisher)	CUCMBE IP@	N/A
CUCM (1 Publisher + 1 Subscriber)	Local redundancy Subscriber (Nominal) / Publisher (Backup) Publisher and Subscriber are on different servers)	Subscriber IP@	Publisher IP@
CUCM (1 Publisher + 2 Subscribers) Subscribers Nominal/Backup	- Local redundancy Subscriber1 (Nominal) / Subscriber2 (Backup) - If more than 1 Subscriber, the SIP trunks are held by the Subscribers. The Publisher holds the database.	Subscriber1 IP@	Subscriber2 IP@
CUCM (1 Publisher + 2 Subscribers) Subscribers Load Sharing	- Local redundancy and Load Sharing Subscriber1 / Subscriber2 - The Subscribers share the load in a round robin fashion (Also applicable with N Subscribers)	Subscriber1 IP@ Subscriber2 IP@	N/A
CUCM with clustering over WAN (1 Publisher + 1 Subscriber)	- Site redundancy: Subscriber and Publisher servers hosted by 2 different physical sites	Subscriber IP@	Publisher IP@
CUCM with clustering over WAN (1 Publisher + 2 Subscribers) Subscribers Nominal/Backup	- Site redundancy: the 2 Subscribers are hosted by 2 different physical sites (Subscriber1(Nominal) / Subscriber2(Backup)) - If more than 1 Subscriber, the SIP trunks are held by the Subscribers. The Publisher holds the database.	Subscriber1 IP@	Subscriber2 IP@
CUCM with clustering over WAN (1 Publisher + 2 Subscribers) Subscribers Load Sharing	- Site redundancy: the 2 Subscribers are hosted by 2 different physical sites (Subscriber1 + Subscriber2) - The Subscribers share the load in a round robin fashion	Subscriber1 IP@ Subscriber2 IP@	N/A
		Nominal	Backup
Remote site without survivability	No survivability, no trunk redundancy	N/A	N/A
SRST	Local site survivability and trunk redundancy via PSTN only	N/A	N/A

3.2 CUCM with CUBE (flow through)

Head Quarter (HQ) or Branch Office (BO) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
CUCM + Single CUBE	No redundancy	CUBE IP@	N/A
CUCM + 2 CUBES **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd CUBE in case both CUBEs are based on different sites	**- Local redundancy:** if both CUBES are hosted by the same site (CUBE1+CUBE2) **- Geographical redundancy:** if each CUBE is hosted by different sites (CUBE1+CUBE2)	CUBE1 IP@	CUBE2 IP@
		Nominal	Backup
Remote site without survivability	No survivability, no trunk redundancy	N/A	N/A
SRST	Local site survivability and trunk redundancy via PSTN only	N/A	N/A

3.3 CUCM with Oracle SBC

Head Quarter (HQ) or Branch Office (BO) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
CUCM + Oracle SBC	No redundancy	Oracle IP@	N/A
CUCM + 2 Oracle SBC Nominal / Backup mode	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	Oracle IP@	Oracle2 IP@
CUCM + 2 Oracle SBC Load Sharing	- **Local redundancy**: both SBC are hosted on the same site OR - **Geographical redundancy** both SBC are hosted on 2 different sites	Oracle IP@	Oracle2 IP@
CUCM + 2 Customer SBC HA mode	- **Local redundancy:** both SBC are hosted on the same site OR **- Geographical redundancy** both SBC are hosted on 2 different sites **warning:** Link level 2 between SBC with max delay 50ms required for geo-redundancy	Oracle Virtual IP@	N/A

3.4 BToI & BTIPoI

Head Quarter (HQ) or Branch Office (BO) architecture	Level of Service	Customer IP addresses used by service	
		Nominal	Backup
CUCM + Single CUBE	No redundancy	CUBE public FQDN* DNS type A	N/A
CUCM + 2 CUBES **warning:** - Site access capacity to be sized adequately on the site carrying the 2nd CUBE in case both CUBEs are based on different sites	**- Local redundancy:** if both CUBES are hosted by the same site (CUBE1+CUBE2) **- Geographical redundancy:** if each CUBE is hosted by different sites (CUBE1+CUBE2)	CUBE1 public FQDN* DNS type A	CUBE2 public FQDN* DNS type A

*BTIPoI can be reached using FQDN only, whereas BToI can be reached either via FQDN or public IP address.

3.4.1 Preliminary configuration

In order to establish the connection with public interface of A-SBC, several preliminary configuration steps have to be performed not related to CUBE configuration. These involve the following:

- Public IP address assignment
- Public DNS record
- Firewall updates
- Certificate updates

3.4.1.1 Public IP address assignment

The certified solution is using a public IP address directly configured on CUBE interface placed within DMZ. It is possible to use NAT address translation since public IP addresses can be limited, however this is not part of standard configuration and require additional modifications to be included on CUBE. Such setup would require a study and validation on customer's request.

3.4.1.2 Public DNS record

Orange A-SBC can be reached via Fully Qualified Domain Name (FQDN) deployed on public DNS. Customer premises CUBE requires records on public DNS that enable to reach it using FQDN via public internet. BTIPoI can be reached using FQDN only, whereas BToI can be reached either via FQDN or public IP address.

- BTIPoI supports type SRV & type A for DNS resolution and do not support direct public IP connections.
- BToI supports both public IP and type A for DNS resolution and do not provide any type SRV record connections.

3.4.1.3 Firewall updates

Firewalls in the way of traffic between CUBE and A-SBC have to be updated in order to open required ports. BToI and BTIPoI vary concerning the UDP port range.

The media UDP port ranges required by Orange BTIPoI SIP Trunk is 6000-38000 and for Orange BToI SIP Trunk is 6000-20000.

CUBE media source ports can be configured within a range of 8000- 48198.

BTIPoI/BToI port matrix				
Source device	Source ports	Destination device	Destination ports	Purpose
CUBE public @IP	TCP 1024-65535	A-SBC public @IP	TCP 5061	TLS SIP signaling
A-SBC public @IP	TCP Any	CUBE public @IP	TCP 5061	
CUBE public @IP	BTIPoI: UDP 8000-38000 BToI: UDP 8000-20000	A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	SRTP media
A-SBC public @IP	BTIPoI: UDP 6000-38000 BToI: UDP 6000-20000	CUBE public @IP	BTIPoI: UDP 8000-38000 BToI: UDP 8000-20000	

3.4.1.4 Certificate updates

In order to ensure the security of traffic, certificates need to be aligned between CUBE and Orange A-SBC. CUBE would require a certificate signed by a public certificate authority and root

CA certificate (including any intermediate certificates in the path). This is described in detail in CUBE secure configuration. The customer should retrieve OBS Root/Intermediate certificates and import those in case of using a different Public Certificate Authority on their side. This is described in detail in CUBE secure configuration.

3.4.1.5 TLS cipher suites support

The following cipher suites are supported by Orange SBC for TLS 1.3 and TLS 1.2.

TLS 1.3:
- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)

TLS 1.2:
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

Currently, Cisco CUBE supports the following cipher suites that are compliant with Orange SBC. At least one cipher suite must be aligned in order for BToI/BTIPoI to work.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Full list of cipher suites supported by CUBE for TLS 1.2 can be found below:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA1
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA (IOS 17.3.1a or later)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (IOS 17.3.1a or later)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (IOS 17.3.1a or later)

3.4.1.6 Sizing guidelines

The below table displays the sizing guidelines provided by Cisco concerning the impact of RTP-SRTP transcoding running on CUBE. For more details please refer to the VISIT CUBE configuration guide.

Platform 1CSR1Kv - Based on tests using Cisco UCS ® C240 host with Intel ® Xeon ® 6132 2.60GHz processors running VMware ESXi 6.0.	Session Capacity (IOS-XE 16.12+) RTP(G711)-RTP(G711)	Impact of sRTP to IPT	Encrypted Audio calls w/GCM256	CPS (Calls per second)

			sRTP(G711)-RTP(G711)	
1100 series (Default DRAM)	500	40%	300	2
4321 (4 GB)	500	40%	300	2
4331 (4 GB)	1000	40%	600	4
4351 (4 GB)	2000	62.5%	750	4
4431 (8 GB)	3000	75%	750	4
4451 (8 GB)	6000	65%	1080	6
4461 (8 GB)	10000 (17.2.1r)	46%	5400 (17.3.1)	30
C8200L-1N-4T (4 GB)	1500 (17.5.1)	67%	500 (17.5.1)	3
C8200-1N-4T (8 GB)	2500 (17.4.1)	68%	800 (17.4.1)	5
C8300-1N1S-6T (8 GB)	7000 (17.3.2)	74%	1800 (17.3.2)	10
C8300-2N2S-6T (8 GB)	7500 (17.3.2)	72%	2100 (17.3.2)	12
C8300-1N1S-4T2X (8 GB)	8000 (17.3.2)	71%	2300 (17.3.2)	13
C8300-2N2S-4T2X (16 GB)	10000 (17.3.2)	52%	4800 (17.3.2)	27
C8000V-S/CSR1Kv – 1 vCPU1 (4 GB)	1000	70%	300	1
C8000V-M/CSR1Kv - 2 vCPU1 (4 GB)	3000	67%	1000	6
C8000V-L/CSR1Kv - 4 vCPU1 (8 GB)	6000	82%	1080	6
ASR1001-X (16 GB)	12000	83%	2000	10
ASR1002-X (16 GB)	14000	68%	4500	25

ASR1004/6/6-X RP2/ESP40 (16 GB)	16000	83%	2700	15

4 Certified software and hardware versions

4.1 CUCM certified versions

Cisco IPBX			
Equipment	Equipment Version	validation status	IPBX Version
CUCM CBE5000/6000	R12.0	✓	Load 12.0.1.21900-7 min
	R12.5	✓	Load 12.5.1.10000-22 min
	R14.0	✓	Load 14.0.1.11900-132 min
	R15.0	✓	Load 15.0.1.11900-23

4.2 Cisco Unified Border Element (CUBE) certified versions

Cisco Unified Border Element (CUBE)					
Equipment		Equipment Version	validation status	IPBX Version	Comment
CUBE - flow-through mode	BVPN	16.6.3	✓	R12.0	
		17.3.4	✓	R12.5	
		17.9.3a	✓	R14.0	
		17.9.3a	✓	R15.0	
	BToI & BTIPoI	17.9.3a	✓	R12.5	
			✓	R14.0	
CUBE – flow-around mode	BVPN	16.6.3	✓	R12.0	BToI and BTIPoI are not supported in flow-around mode
		17.3.4	✓	R12.5	
		17.9.3a	✓	R14.0	
		17.9.3a	✓	R15.0	

4.3 Oracle ESBC certified versions

Oracle ESBC				
Equipment	Equipment Version	validation status	IPBX Version	Comment
Oracle Enterprise Session Border Controller	8.2 Patch 2 (Build 58)	✓	R12.0	

4.4 CUCM certified applications and devices versions

Cisco ecosystems					
Equipment		Equipment Version	validation status	IPBX Version	Comment
Attendant Console	CUxAC	12.0.x	✓	R12.x	Standard and Advanced editions
		14.0	✓	R14.0	Standard and Advanced editions
		15.0	✓	R15.0	Standard and Advanced editions

Voice Mail	Unity Connection	12.0.1000-6	✓	R12.0	
		12.5	✓	R12.5	
		14.0	✓	R14.0	
		15.0	✓	R15.0	
	Unity Express	12.0.x	✓	R12.0	

Contact center	UCCX	12.0.x	✓	R12.0	
		12.5.1SU2	✓	R14.0	

MGW	Cisco IOS Cascaded MediaGateway (ISR 28xx/38xx)		not supported	R14.0	
	Cisco IOS Cascaded MediaGateway (ISR 29xx/39xx)	15.7(3)M	✓	R12.x	SIP Fax and analog phone supported
				R14.0	
	Cisco IOS Cascaded MediaGateway (ISR 43xx/44xx)	16.6.3	✓	R12.0	SIP Fax and analog phone supported
		17.6.4	✓	R12.5	
		17.9.3a	✓	R14.0	
		17.9.3a	✓	R15.0	
	Analog GW Cisco ATA191	12-0-1SR2-3	✓	R12.5	Analog phone supported. SIP Fax unstable.
		12-0-1-0301-002	✓	R14.0	
	Audiocodes MP112 FXS		on demand	R14.0	
	Analog GW Cisco VG 224		not supported	R14.0	
	Analog GW Cisco VG 202-204		not supported	R14.0	
	Analog GW Cisco VG 202-204 XM	15.5(3)M2	✓	R12.x	SIP Fax and analog phone supported
	Analog GW Cisco VG 310-320-350	15.7(3)M	✓	R12.x	SIP Fax and analog phone supported
	Analog GW Cisco VG 450	17.6.4	✓	R12.5	SIP Fax and analog phone supported
			✓	R14.0	SIP Fax and analog phone supported
	Analog GW Cisco ATA190	1.2.1(004)	✓	R12.0	SIP Fax and analog phone supported
		1.2.2(003)	✓	R12.5	

VOIP	Cisco VoIP GW		on demand	R14.0	
	OneAccess VoIP GW (Business Livebox)		on demand	R14.0	

Phones	Cisco Unified Communication Manager Assistant (IPMA)		not supported	R14.0	
	All Cisco SCCP phones (skinny)		✓	R14.0	

			✓	R15.0	
	All Cisco SIP phones		✓	R14.0	
	IPCommunicator SCCP		not supported	R14.0	
	Jabber	14.0	✓	R14.0	
	Jabber	14.3	✓	R15.0	
	IP DECT ASCOM		✓	R12.x	

Third Party Equipments	Conecteo KIAMO	6.1	✓	R11.x R12.0	Dorsal mode

5 Cisco Call Manager configuration

The checklists below present all the configuration steps required for interoperability between the service and CUCM.

Cisco Call Manager Service **Codec and payload configuration**	
Menu	**Value**
System > Service Parameters > Appropriate server > Cisco CallManager (Active) > Advanced > Clusterwide Parameters (System – Location and Region)	
Preferred G.711 Millisecond Packet Size	20
Preferred G.729 Millisecond Packet Size	20
G.722 Codec Enabled	Enabled for All Devices
Cisco CallManager Service **Codec and payload configuration**	
System > Service Parameters > Appropriate server > Cisco CallManager (Active) > Advanced Clusterwide Parameters (Service)	
Duplex Streaming Enabled	True
Media Exchange Timer	5
Silence suppression	False
Silence suppression for Gateways	False
Media Exchange Timer	True
Cisco CallManager Service **SIP Parameters**	
System > Service Parameters > Appropriate server > Cisco CallManager (Active) > Advanced Clusterwide Parameters (Device - SIP)	
Retry Count for SIP Invite	1
SIP Session Expires Timer	86400
Cisco CallManager Service **System – QOS Parameters**	
System > Service Parameters > Appropriate server > Cisco CallManager (Active) > Advanced Clusterwide Parameters (System - QOS)	
DSCP for Video Calls	34 (100010)
Cisco CallManager Service **Enterprise Parameters**	
System > Enterprise Parameters	
Advertise G.722 Codec	Enabled
Cisco CallManager Service **Cisco IP Voice Media Streaming Application service**	
System > Service Parameters > Appropriate server > Cisco IP Voice Media Streaming App (Active)	
MTP Run Flag	False
Supported MOH Codec	G711alaw/G711ulaw, G729 Annex A

<table>
<tr><th colspan="2"><b>Cisco CallManager Service</b>
Region configuration</th></tr>
<tr><th>Menu</th><th>Value</th></tr>
<tr><td colspan="2">System > Region Information > Region</td></tr>
<tr><td>Regions configuration for customer using G.729</td><td>
<table>
<tr><th>From
To</th><th>HQ</th><th>RS</th><th>WAN</th></tr>
<tr><td>HQ</td><td><b>G711</b></td><td>G729</td><td>G729</td></tr>
<tr><td>RS</td><td>G729</td><td><b>G711</b></td><td>G729</td></tr>
<tr><td>WAN</td><td>G729</td><td>G729</td><td>G729</td></tr>
</table>
</td></tr>
<tr><td>Regions configuration for customer using G.711</td><td>
<table>
<tr><th>From
To</th><th>HQ</th><th>RS</th><th>WAN</th></tr>
<tr><td>HQ</td><td><b>G711</b></td><td>G711</td><td>G711</td></tr>
<tr><td>RS</td><td>G711</td><td><b>G711</b></td><td>G711</td></tr>
<tr><td>WAN</td><td>G711</td><td>G711</td><td>G711</td></tr>
</table>
</td></tr>
<tr><th colspan="2"><b>Cisco CallManager Service</b>
Device Pool Configuration</th></tr>
<tr><td colspan="2">System > Device Pool > Add new</td></tr>
<tr><td>New Device Pool</td><td>Device Pool configuration:
• The number of Device Pools at least should be the same as the number of site
• Every Device Pool should have appropriate Region and Location value

<b>Note:</b> MOH server requires a separate Device Pool configuration.</td></tr>
<tr><th colspan="2"><b>Cisco CallManager Service</b>
Locations (Call Admission Control)</th></tr>
<tr><td colspan="2">System > Location Info> Location > Add new</td></tr>
<tr><td>New Location</td><td><b>Warning!</b> RSVP locations are not supported!

Create the necessary locations and configure the bandwidth for each.</td></tr>
</table>

Media Resources

Transcoder configuration : Warning! Hardware MTP resources on IOS Gateway and software MTP resource on CUCM are NOT SUPPORTED. Software MTPs on IOS Gateway are SUPPORTED in BT/BTIP SIP Trunking.

Menu	**Value**
Media Resources > Transcoder > Add new	
Transcoder Type	Cisco IOS Enhanced Media Termination Point
Device Name	Use the name configured in sccp ccm group in the IOS
Device Pool	Use the appropriate Device Pool
Trusted Rely Point	Unchecked
Media Resources Conference Bridge configuration	
Media Resources > Conference Bridge > Add new	
Conference Bridge Type	Cisco IOS Enhanced Media Termination Point
Device Name	Use the name configured in sccp ccm group in the IOS
Device Pool	Use the appropriate Device Pool
Device Security Mode	Non Secure Conference Bridge
Media Resources Multicast Music on Hold CUCM configuration - Region	
System > Region Information > Region > Add new	
New Region	Please refer to chapter on Region configuration for additional information. With this configuration, all devices in “MoH Multicast” region will use G.711 as codec for sending RTP packets to devices to all other regions and also for the “WAN” region where codec G.711 will be used.
Media Resources Multicast Music on Hold CUCM configuration – Device Pool	
System > Device Pool > Add new	
New Device Pool	Choose a name and associate the Region “MoH Multicast” to this new Device Pool.
Media Resources Multicast Music on Hold CUCM configuration - Audio Source Configuration	
Media Resources > Music On Hold Audio Source > Add new	
Play continuously (repeat)	Checked
Allow Multicasting	Checked

Media Resources Multicast Music on Hold CUCM configuration - Multicast MoH server configuration	
Menu	**Value**
Media Resources > Music On Hold Server	
Device Pool	Checked
Enable Multi-cast Audio Sources on this MoH Server	Checked
Base Multi-cast IP Address	239.1.1.1 *(example)*
Base Multi-cast IP Port	16384 *(example)*
Increment Multi-cast on	IP Address
Max Hops (per Audio Source in Selected Audio Sources configuration area)	1
Media Resources Multicast Music on Hold CUCM configuration - Multicast MoH server configuration	
Media Resources > Media Resource Group	
Appropriate Media Resource Group	Check the Use Multicast for MoH Audio checkbox to allow multicast with this resource group.
Media Resources Multicast Music on Hold Router configuration – Audio file	
Frequency	9kHz
Coded with	8bit
Audio mode	Mono
Codec type	CCITT u-law
Media Resources Multicast Music on Hold Router configuration – IOS Commands	

Commands	ccm-manager music-on-hold
	call-manager-fallback
	  max-conferences 4
	  ip source-address 10.108.105.254 port 2000
	  max-ephones 24
	  max-dn 48
	  moh TheJourneyAndTheWind.alaw.wav
	  multicast moh 239.1.1.1 port 16384 route 210.72.240.13 10.108.105.254

Media Resources Multicast Music on Hold Media Resource Group Lists configuration	
Media resources	**Warning!** Media Resources, which are not associated with any MRG are available to every device in the cluster by default. Media Resources > Media Resource Group > Add new Resources > Media Resource Group List > Add new

Off-net calling via BT/BTIP Diversion Header manipulation Partition	
Menu	**Value**
Call Routing -> Class of Control -> Partition -> Add new	
Name	DIV-HEADER-PT
Off-net calling via BT/BTIP Diversion Header manipulation Called Party Transformation Pattern	
Call Routing -> Transformation -> Transformation Pattern -> Called PartyTransformation Pattern -> Add New	
Pattern	XXXX
Prefix digits	Site Prefix
Off-net calling via BT/BTIP Diversion Header manipulation Calling Search Space	
Call Routing -> Class of Control -> Calling Search Space -> Add New	
Name	DIV-HEADER-CSS
Selected Partitions	DIV-HEADER-PT
Off-net calling via BT/BTIP Basic Configuration Sip Trunk Security Profile	
System > Security > SIP Trunk Security Profile, select “Non Secure SIP Trunk Profile” from SIP Trunk Security Profile List	
Incoming Transport Type	TCP + UDP
Outgoing Transport Type	UDP
Off-net calling via BT/BTIP Basic Configuration SIP Profile	
Device > Device Settings > SIP Profile	
User-Agent and Server header information	Send Unified CM Version Information as User-Agent Header
Version in User Agent and Server Header	Full Build
SIP Rel1XX Options	Send PRACK for 1xx Messages
Early Offer support for voice and video	Mandatory (insert MTP if needed)
Send send-receive SDP in mid-call INVITE	Checked
Ping Interval for In-service and Partially In-service Trunks (seconds)	300
Ping Interval for Out-of-service Trunks (seconds)	5
Version in User Agent and Sever Header	Full build
Session Refresh Method	INVITE or UPDATE

Version in User Agent and Sever Header - inject info about full version of CUCM

Session Refresh Method - since CUCM 10.0 there is additional method – “UPDATE”. “INVITE” should be used by default.

Off-net calling via BT/BTIP

Basic Configuration

SIP Normalization Script

Device > Device Settings > SIP normalization script > Add new

```
SIP Normalization Script is applied to SIP trunk and is required to adapt
the SIP signaling to the form expected by BT/BTIP infrastructure.
The content of the  script is given below:
```

```
-- Orange SIP Normalization Script v11
-- this is normalization script for uc 12.x or later
M = {}


-- This is called when an INVITE message is sent
function M.outbound_INVITE(msg)
    local sdp = msg:getSdp()
    if sdp
    then
       -- remove b=TIAS:
       sdp = sdp:gsub("b=TIAS:%d*\r\n", "")
       -- store the updated sdp in the message object
       msg:setSdp(sdp)
    end
end


--modifying of Server header in 183 messages
function M.outbound_183_INVITE(msg)
-- change 183 to 180 if sdp
 local sdp = msg:getSdp()
 if sdp
 then
  msg:setResponseCode(180, "Ringing")
 end
end

--modifying of Server header in 488 messages
function M.outbound_488_INVITE(msg)
 -- change 488 to 503 if sdp
  msg:setResponseCode(503, "Service Unavailable")
end

--handling of 400 errors
function M.inbound_400_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
```

```
  msg:addHeader("Reason", "Q.850; cause=27")
 end
end

--handling of 403 errors
function M.inbound_403_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 408 errors
function M.inbound_408_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 480 errors
function M.inbound_480_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=20")
 end
end

--handling of 481 errors
function M.inbound_481_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
  msg:addHeader("Reason", "Q.850; cause=27")
 end
end

--handling of 487 errors
function M.inbound_487_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=16")
 end
end

--handling of 488 errors
function M.inbound_488_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=127")
 end
```

```
end

--handling of 500 errors
function M.inbound_500_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 501 errors
function M.inbound_501_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 502 errors
function M.inbound_502_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 503 errors
function M.inbound_503_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 505 errors
function M.inbound_505_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 513 errors
function M.inbound_513_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- addition of PAI header if incoming INVITE includes Privacy
header
function M.inbound_INVITE(msg)
 -- get Privacy header
 local privacy = msg:getHeader("Privacy")
 if privacy
 then
  -- get From and Pai
  from = msg:getHeader("From")
  pai = msg:getHeader("P-Asserted-Identity")
  --check if Pai header is not present
  if pai==nil
  then
   -- add Pai header filled with From URI value
   local uri = string.match(from, "(<.+>)")
   msg:addHeader("P-Asserted-Identity", uri)
  end
 end
end

return M
```

Off-net calling via BT/BTIP Basic Configuration SIP Trunk Configuration	
Menu	**Value**
Device > Trunk > Add new	
Device Pool	Choose Device Pool which include Region and Location value
Media Resource Group List	MRGL
Redirecting Diversion Header Delivery - Inbound	Checked
Redirecting Diversion Header Delivery - outbound	Checked
Destination Address	SBC IP Address
SIP Trunk Security Profile	SIP Trunk Security Profile name
SIP Profile	Standard SIP Profile with PRACKs, EO, Send-recv
DTMF Signaling Method	RFC 2833
Normalization Script	SIP Normalization Script name (currently v8)
Enable Trace	Unchecked
Redirecting Party Transformation CSS	DIV-HEADER-CSS
Off-net calling via BT/BTIP Basic Configuration Route Group	
Call Routing > Route/Hunt > Route group > Add new	
Distribution algorithm	Top Down
Selected devices	both SIP trunks to ORACLE/ACMEs
Off-net calling via BT/BTIP Basic Configuration Route List	
Call Routing > Route/Hunt > Route list > Add new	
Selected Groups	Route Group with SIP trunks to BT/BTIP
Off-net calling via BT/BTIP Basic Configuration Route Pattern	
Call Routing > Route/Hunt > Route Pattern > Add new	
Route Pattern	Specific Route Pattern
Gateway/Route List	Route List name
Call Classification	OffNet
Discard Digits	PreDot Trailing#
On-net calling Basic Configuration	
The configuration of such intercluster SIP Trunk is the same as the one described for off-net calls except that on trunk between sites there is no SIP Normalization Script.	
SME Architecture (ON CUSTOMER DEMAND) Off-net calling via BT/BTIP	

SIP Trunk Security Profile (at CUCM SME and CUCM)	
Menu	**Value**
System > Security > SIP Trunk Security Profile > Add new	
Incoming Transport Type	TCP + UDP
Outgoing Transport Type	UDP
SME Architecture Off-net calling via BT/BTIP SIP Trunk Security Profile (at CUCM SME and CUCM)	
Device > Device Settings > SIP Profile	
User-Agent and Server header information	Send Unified CM Version Information as User-Agent Header
Version in User Agent and Server Header	Full Build
SIP Rel1XX Options	Send PRACK for 1xx Messages
Early Offer support for voice and video calls (insert MTP if needed)	Checked
Send send-receive SDP in mid-call INVITE	Checked
Ping Interval for In-service and Partially In-service Trunks (seconds)	300
Ping Interval for Out-of-service Trunks (seconds)	5
SME Architecture Off-net calling via BT/BTIP SIP Normalization Script (at CUCM SME)	
Device > Device Settings > SIP normalization script > Add new	

SIP Normalization Script is applied to SIP trunk at CUCM SME and is required to adapt the SIP signaling to the form expected by BT/BTIP infrastructure. Create the script.
The content of the script is given below:

```
-- Orange SIP Normalization Script v11
-- this is normalization script for uc 12.x or later
M = {}


-- This is called when an INVITE message is sent
function M.outbound_INVITE(msg)
    local sdp = msg:getSdp()
    if sdp
    then
       -- remove b=TIAS:
       sdp = sdp:gsub("b=TIAS:%d*\r\n", "")
       -- store the updated sdp in the message object
       msg:setSdp(sdp)
    end
end


--modifying of Server header in 183 messages
function M.outbound_183_INVITE(msg)
-- change 183 to 180 if sdp
 local sdp = msg:getSdp()
 if sdp
 then
  msg:setResponseCode(180, "Ringing")
 end
end

--modifying of Server header in 488 messages
function M.outbound_488_INVITE(msg)
 -- change 488 to 503 if sdp
  msg:setResponseCode(503, "Service Unavailable")
end

--handling of 400 errors
function M.inbound_400_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
  msg:addHeader("Reason", "Q.850; cause=27")
 end
end

--handling of 403 errors
function M.inbound_403_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 408 errors
function M.inbound_408_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 480 errors
function M.inbound_480_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=20")
 end
end

--handling of 481 errors
function M.inbound_481_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
  msg:addHeader("Reason", "Q.850; cause=27")
 end
```

```
end

--handling of 487 errors
function M.inbound_487_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=16")
 end
end

--handling of 488 errors
function M.inbound_488_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=127")
 end
end

--handling of 500 errors
function M.inbound_500_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 501 errors
function M.inbound_501_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 502 errors
function M.inbound_502_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 503 errors
function M.inbound_503_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
```

```
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 505 errors
function M.inbound_505_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 513 errors
function M.inbound_513_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- addition of PAI header if incoming INVITE includes Privacy
header
function M.inbound_INVITE(msg)
 -- get Privacy header
 local privacy = msg:getHeader("Privacy")
 if privacy
 then
  -- get From and Pai
  from = msg:getHeader("From")
  pai = msg:getHeader("P-Asserted-Identity")
  --check if Pai header is not present
  if pai==nil
  then
   -- add Pai header filled with From URI value
   local uri = string.match(from, "(<.+>)")
   msg:addHeader("P-Asserted-Identity", uri)
  end
 end
end

return M
```

SME Architecture Off-net calling via BT/BTIP SIP Trunk Configuration to offnet (at CUCM SME)	
Menu	**Value**
Device > Trunk > Add new	
Device Pool	Choose Device Pool which include Region and Location value

Media Resource Group List	None
Redirecting Diversion Header Delivery - Inbound	Checked
Destination Address	SBC IP Address
SIP Trunk Security Profile	SIP Trunk Secure Profile name
SIP Profile	Standard SIP Profile with PRACKs, EO and Send-recv
Normalization Script	SIP Normalization Script name
Enable Trace	Unchecked
SME Architecture Off-net calling via BT/BTIP Route group (at CUCM SME)	
Call Routing > Route/Hunt > Route group > Add new	
Distribution algorithm	Top Down
Selected devices	both SIP trunks to ORACLE/ACMEs
SME Architecture Off-net calling via BT/BTIP Route list (at CUCM SME)	
Call Routing > Route/Hunt > Route list > Add new	
Selected Groups	Route Group with SIP trunks to BT/BTIP
SME Architecture Off-net calling via BT/BTIP Route pattern (at CUCM SME)	
Call Routing > Route/Hunt > Route Pattern > Add new	
Route Pattern	Specific Route Pattern
Gateway/Route List	Route List name
Call Classification	OffNet
Discard Digits	PreDot Trailing#

SME Architecture On-net calling	
The configuration of such intercluster SIP Trunk is the same as the one described for off-net calls except for: • Media Resource Group List – should be set to the group containing following resources: conference, transcoder, annuciator (Subscribers), MOH Server (Subscribers), software MTP • SIP Normalization Script should not be added to this trunk SIP Trunks should be between CUCM of independent site and CUCM SME (there is no direct SIP Trunks between independent sites in SME Architecture – all on-net calls are managed by CUCM SME).	
Emergency number support for Extension Mobility Partitions	
Menu	**Value**
Call Routing > Class of Control > Partition > Add new	Create a partition for emergency numbers for each site, for example: EN_HQ_PT, EN_RSA_PT, EN_RSB_PT.
Route Patterns	
Call Routing > Route/Hunt > Route Pattern > Add new	
Route Partition	Choose Partition for appropriate Route Pattern
Urgent Priority	Checked
Calling Party Transform Mask	Enter valid office attendant phone number (unique for each site)
Calling search spaces	
Call Routing > Class of Control > Calling Search Space > Add new	
Create a CSS for emergency numbers for each site and another one for non-emergency numbers. ❶ CSS_LINE associated to the line deals with general call right except emergency numbers. ❷ CSS_PHONE associated to the phone deals with emergency calls. This CSS should be unique for each site.	
Device > Phone > Calling Search Space	
Associate the calling search spaces for emergency numbers with particular phones (deivces), and calling search spaces for non-emergency numbers with lines.	
Device > Phone -> find a phone ->Calling Search Space field	select the proper CSS
Device > Phone -> find a phone ->select the line on the left menu -> Calling Search Space field	select the proper CSS
Survivable Remote Site Telephony configuration	
SRST mode is not supported with BT/BTIP infrastructure but with local PSTN gateway configured on CE router	

6 Cisco Unity Connection configuration

Cisco Unified Communication Manager Configuration	
Menu	**Value**
System > Device Pool > Add New	Add new Device pool
Advanced FeaturesVoice Mail > Cisco Voice Mail Port Wizard >	Create a new Cisco Voice Mail Server and add ports to it
Call Routing > Route/Hunt > Line Group	add/configure the Answering Voice Mail Ports to a Line Group
Call Routing > Route/Hunt > Hunt List > Add New	include the Line Group created earlier
Call Routing > Route/Hunt > Hunt Pilot > Add New	include the Hunt List created earlier
Advanced Features > Voice Mail > Message Waiting	add one number for turning MWIs on and one for turning MWIs off
Advanced Features > Voice Mail > Voice Mail Pilot > Add New	Configure the voice mail pilot
Advanced Features > Voice Mail > Voice Mail Profile > Add New	Associate Voice Mail Pilot number created earlier with this profile
Cisco Unity Connection Configuration	
Telephony Integrations > Phone System	Configure the phone system
Phone System Basics > Related Links drop-down box > Add Port Group > Go	Port group configuration
Port Group Basics > Related Links drop-down box > Add Ports > Go	Add and configure required number of ports
Cisco Unity Connection Administration > Telephony Integrations > Port Group	On Search Port Groups page click the display name of the port group that you created with the phone system integration
Port Group Basics page > Edit > Servers >	add backup CUCM servers if needed
BT/BTIP specific parameters	
Telephony Integrations -> Port Group -> choose appropriate -> Edit -> Codec Advertising	change the codec list used for calls to CUC - select G.711 A-law / G.711ulaw/G.722 or G.729 codecs in advertised codecs.
System Setting > General Configuration	Select G.711 a-law, G.711 u-law or G.729 codec as specified for Recording Format parameter

7 Unified Contact Center Express configuration

7.1 Provisioning UCCX (CUCM part)

7.1.1 Adding agents

Unified CM users in Unified CCX are assigned an agent's role when an **agent extension** is associated to the user in the Unified CM User Configuration page. Consequently, this role can only be assigned or removed for the user using Unified CM Administrator's End User configuration web page. These users cannot be assigned or removed in Unified CCX Administration.

Configuring Unified CM users who will be agents in your Unified CCX system:

Step 1 From the **Unified CM Administration** menu bar, choose **User Management > End User**.

Step 2 In the **Controlled Devices** list box below the Device Information section, select the agent's phone device.

Step 3 In the **Primary Extension** field drop-down list and the **IPCC Extension field** drop-down list, choose the required agent extension for this device.

Step 4 Define permissions and roles information:

Groups:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard CTI Allow Call Monitoring
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled
- Standard Confidential Access Level Users

Roles:

- Standard AXL API Access
- Standard CCM Admin Users
- Standard CTI Allow Call Park Monitoring
- Standard CTI Allow Call Recording
- Standard CTI Allow Calling Number Modification
- Standard CTI Allow Control of All Devices

- Standard CTI Enabled
- Standard CUReporting
- Standard CUReporting Authentication
- Standard Confidential Access Level Users

Step 5 Adding End User to IP phone - End user related to UCCX has to be associated to ip phone profile and ip phone line

7.1.2 Activation and Configuring IP Phone Agent service

Step 1 Activate IP Phone Agent service (URL can be found in CAD administration guide: **http://UCCX_IP_address or FQDN:8082/fippa/#DEVICENAME#**): CUCM administration > Device > Device Settings > Phone services

Step 2 Create parameters which will be used to log in IP Phone Agent service: extension, id and password.

Step 3 Subscribe agent phone to this newly created service (Phone > Subscribe services drop-box list)

Step 4 (Optional, if needed) Create an application user named “telecaster” with “telecaster” as the password (or whatever BIPPA user ID and password was specified in the CAD Configuration Setup utility).

Step 5 (Optional, if needed) Assign the telecaster application user to all the IP agent phones

7.1.3 UCCX Application Users on CUCM

When UCCX will be properly configured **two Application Users should be created automatically on CUCM**:

- RMCM user

  Go to CUCM administration > User Management > Application User > RMCM user

  IP Phone (which will be used as the agent) manually associates with “Device Association” to RMCM user Controlled Device.

- JTAPI user

  Go to CUCM administration > User Management > Application User > JTAPI user

  Automatic creation of this user should take place on CUCM **(after proper configuration of UCCX)** and then UCCX CTI ports should appear automatically in the list “Controlled Devices”.

7.2 UCCX part of configuration

7.2.1 Provisioning Call Control Group (CCC)

Provision Unified CM Telephony call control groups (**Subsystems > Unified CM Telephony > Call Control Group**). They are CTI ports which will be used by UCCX to handle calls

- Define Description
- Define Number of CTI Ports
- Define Name Prefix
- Define Starting Directory Number – unique and not used on CUCM
- Define Device Pool
- (optionally – if needed) Synchronize Cisco JTAPI Client and Unified CM Telephony Data (this creates all necessary CTI devices on CUCM using AXL interface)

Note! Correct behavior - CTI ports should be created and assigned automatically into CCC. CTI ports should be also automatically created and registered on CUCM via AXL integration. If not then perform step 6.

7.2.2 Resources and assignment of skills

Step 1 Check if resources exist – it should exist if former steps of configuration on CUCM and UCCX were performed properly (**Subsystems > RmCm > Resources**)

Step 2 Create skills (**Subsystems > RmCm > Skills**)

Step 3 Choose Resource Name and click Add Skill (**Subsystems > RmCm > Assign Skills**).

Step 4 Assigning skills to agents

Before assigning the skill competence level of the skill should be defined (default is 5)

7.2.3 Configuring Customer Service Queues (CSQ)

Step 1 Creating Contact Service Queues.(**Subsystems > RmCm > Contact Service Queues**)

Step 2 Define name of CSQ

Step 3 Define type of Resource Pool Selection Model (drop-down list)

Step 4 Click “next” and change default values of parameters of CSQ (if needed), if not just click “update”.

Note! Minimum Competence Level shouldn’t be higher than formerly defined Competence Level during assigning skills into Resources.

7.2.4 Application and Script configuration

Step 1 Add a new Cisco script application, go to: **Applications > Application Management>Add New** and choose Cisco Script Application:

Step 2 From the Application Type drop-down menu select your script or the standard ICD script **SSCRIPT[icd.aef]** and click “Next”

Step 3 Describe maximum number of sessions (should be “inline” with numbers of CTI ports)

Step 4 Mark checkbox CSQ and enter the name.

Step 5 Define Description

7.2.5 Trigger configuration

Step 1 Add a new Trigger, go to: **Applications > Application Management** and choose application from the list.

Step 2 Choose “Add new trigger”

Step 3 Define Trigger Type and click Next

Step 4 Define **unique** directory number and trigger information (don’t forget to assign Call Control Group formerly defined)

Step 5 Perform JTAPI and Data resynchronization (**Subsystems > Cisco Unified CM Telephony**)

Step 6 Check CUCM configuration – CTI Route Point should be automatically created with Trigger number defined on UCCX (**Devices > CTI Route Point**)

Step 7 Check CUCM configuration – this CTI Route Point should be also automatically assigned on JTAPI user (**User Management > Application User**)

8 Cisco Unified Attendant Console configuration

CISCO UNIFIED COMMUNICATION MANAGER	
Device>CTI Route Point>Add New	
Menu	**Value**
User ID	CUDAC
Password	Enter password
Confirm Password	Confirm entered password
User Management > Application User > Add new	
User ID	CUDAC
Password	Enter password
Confirm Password	Confirm entered password
BLF Presence Group	Standard Presence Group
Permissions Information	-Standard Access AXL API -Standard CTI Allow Car Park Monitoring -Standard CTI Allow Calling Number Modification -Standard CTI Allow Control of All Devices -Standard CTI Allow Reception of SRTP Key Material -Standard CTI Enabled -Standard CTI Allow Control of Phones supporting Rollover Mode -Standard CTI Allow Control of Phones supporting Connected Xfer and conf
CISCO UNIFIED ATTENDAND ADMIN	
Menu	**Value**
Installation	• When asked enter the IP address of the machine server is being installed on • If SQL Server Express is already installed enter the SQL Server name, User Name, ale password. If you don't have SQL installed it will be installed automatically • Enter the IP address of CUCM • Enter port number (443) • Enter Application User credentials created before • If certificate security alert from CUCM will be displayed it means connection was successful, accept the certificate • Follow on screen instructions
Database Wizard	• Once installation is completed the database is started, let the wizard to perform necessary configuration, when done, click finish, and restart the computer.
http://<<ip.address.of.Unified.Attendand.Server>>/webadmin/login.aspx	Login to the Attendant Server administration User name: ADMIN Password: CISCO

Engineering > Administrator Management	Let's you change default password
Engineering > Database Management	Parameters for the SQL server, if blank enter IP address of machine where SQL server is installed, specify user name, and password,

Menu	**Value**
Engineering > CUCM connectivity	CUCM parameters, if blank, enter CUCM IP address in name field, port number (443), and user name and password of application user.
Engineering > Database Management	Parameters for the SQL server, if blank enter IP address of machine where SQL server is installed, specify user name, and password of application user
System Configuration > System Device Menagment	
CT Gateway Devices> From	6301 (*example)*
CT Gateway Devices> To	6302 (*example)*
Service Devices> From	6401 (*example)*
Service Devices>To	6402 (*example)*
Park Devices>From	6501 (*example)*
Park Devices>To	6502 (*example)*
System Configuration > System Device Menagment	Synchronize with CUCM (Devices will be added automatically to CUCM)
User Configuration > General Properties	
Minimum internal device digit length	1
Maximum internal device digit length	7
External access number	8
Note! Such configuration is necessary to perform successful delayed transfer. Although etting external access number makes it impossible to perform onnet connections to numbers beginning with 8 (i.e LO BLB) as even though they are seven digits numbers, they are traeted as external numbers. Refer to mantis ticket 2462.	
User Configuration > Queue Management	
Team	Dev1
DDI	6100 (example)
Synchronize with CUCM	Will be automatically added to CUCM as CTI port
User Configuration > Operator Management	
Login Name	OPERATOR1 (example)
Password	Set password
Confirm Password	Confirm password
Associated Queues	Associate queue created in previous step
CISCO UNIFIED ATTENDAND CONSOLE	
Menu	**Value**
Installation	• When asked enter the IP address of Cisco Unified Attendant Server • Select the language for application

	- Follow on screen instruction until installation I completed
Login	Login with credentials created in previous step
CISCO UNIFIED COMMUNICATION MANAGER	
User Management > Application User > CUDAC	
Controlled Devices	Associate devices added by CUDAC Admin
Device > CTI route point > Route point created by CUDAC Admin	
Media Resource Group List	MRGL_MTP_XCODE

9 CUCM with CUBE configuration and SIP Trunk over BVPN (BT/BTIP)

9.1 General Cisco Unified Border Element (CUBE) configuration (flow-through mode by default)

network interface

Note : for two SIP trunks two IP addresses must be configured.

```
interface GigabitEthernet0/0
 description CUBE Voice Interface
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.<INTERFACE>
 description *** CUBE ***
 encapsulation dot1Q <INTERFACE>
 ip address <IP_ADDR> <Mask>
```

SNMP Server

```
snmp-server community public RO
snmp-server manager
```

Global settings

```
voice service voip
      mode border-element license capacity [session count]
      allow-connections sip to sip
      sip
          header-passing
          error-passthru
      pass-thru headers unsupp
          no update-callerid
      early-offer forced
          midcall-signaling passthru
          sip-profiles 1
             ip address trusted list
                    ipv4 A.B.C.D   ! primary SBC IP address
                    ipv4 E.F.G.H   ! backup SBC IP address
```

Codecs

For customers using G.711 alaw codec:

```
voice class codec 1
   codec preference 1 g711alaw
```

For customers using G.711 ulaw codec:

```
voice class codec 1
   codec preference 1 g711ulaw
```

For customers using G.729 codec use following configuration:

```
voice class codec 2
   codec preference 1 g729r8
```

SIP User Agent

```
sip-ua
   retry invite 1
   retry response 2
   retry bye 2
   retry cancel 2
   reason-header override
   connection-reuse
   g729-annexb override
   timers options 1000
```

Support for Privacy and P-Asserted Identity

To enable the privacy settings for the header on a specific dial peer, use the voice-class sip privacy id command in dial peer voice configuration mode:

```
dial-peer voice tag  voip
   voice-class sip privacy id
```

To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the voice-class sip asserted-id pai command in dial peer voice configuration mode:

```
dial-peer voice tag voip
   voice-class sip asserted-id pai
```

9.2 Media Passing through CUBE (media flow-through vs. media flow-around)

Default CUBE configuration enables CUBE to work in flow-through mode. In order to enable flow-around mode, please perform the following actions:

```
voice service voip
   media flow-around
```

9.3 Configuration for a CUCM cluster and two CUBEs

CUBE needs to be configured with physical interface will be configured with a secondary IP address.

```
interface FastEthernet 0/0.<INTERFACE>

   ip address <PRIMARY_IP_ADDR> <Mask>

   ip address <SECONDARY_IP_ADDR> <Mask> secondary
```

CUCM cluster will be configured with 4 different SIP trunks :

- 1st SIP trunk pointing to the primary address of Primary CUBE
- 2nd SIP trunk pointing to the secondary address of Primary CUBE
- 3rd SIP trunk pointing to primary address of Secondary CUBE
- 4th SIP trunk pointing to secondary address of Secondary CUBE

CUCM will be configured with a Route List composed of (at least) 4 Route Groups. Each route group will include SIP trunk to one of CUBE IP Address (Primary or Secondary). On each route group parameters, a specific prefix should be defined (one prefix for each RG). This way the CUBE will be able to route the outgoing calls to the right SBC, depending on this prefix value:

For incoming and outgoing calls for CUCMs side

```
dial-peer voice 1 voip
 description ** to/from site devices - Primary CUCM **
 answer-address <INTERFACE>....
 destination-pattern <INTERFACE>....
 session protocol sipv2
 session target ipv4:<PRIMARY_CUCM_IP_ADDR>
 voice-class codec 1
 voice-class sip options-keepalive up-interval 300 down-interval 300 retry 5
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 2 voip
 description ** to/from site devices - Backup CUCM **
 preference 1
 answer-address <INTERFACE>....
 destination-pattern <INTERFACE>....
 session protocol sipv2
 session target ipv4:<SECONDARY_CUCM_IP_ADDR>
 voice-class codec 1
 voice-class sip options-keepalive up-interval 300 down-interval 300 retry 5
 dtmf-relay rtp-nte
 no vad

!For outgoing calls (with a prefix to select the target SBC)
dial-peer voice 102 voip
 description ** Outgoing calls - Outbound dial peer - Primary SBC side **
 translation-profile outgoing 113
 huntstop
 destination-pattern 113T
 session protocol sipv2
 session target ipv4:<PRIMARY_SBC_IP_ADDR>
 voice-class codec 1
 voice-class sip options-keepalive up-interval 300 down-interval 300 retry 5
 voice-class sip send 180 sdp
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 103 voip
 description ** Outgoing calls - Outbound dial peer - Backup SBC side **
 translation-profile outgoing 114
 huntstop
 destination-pattern 114T
 session protocol sipv2
 session target ipv4:<SECONDARY_SBC_IP_ADDR>
 voice-class codec 1
 voice-class sip options-keepalive up-interval 300 down-interval 300 retry 5
 voice-class sip send 180 sdp
 dtmf-relay rtp-nte
 no vad

!For incoming calls
```

```
dial-peer voice 100 voip
 description ** Incoming calls - Inbound dial peer - SBC side **
 answer-address +.T
 session protocol sipv2
 voice-class codec 1
 voice-class sip send 180 sdp
 dtmf-relay rtp-nte
 no vad
!
```

The prefix should be stripped using voice translation rules before sending the call to the infrastructure.

9.4 Configuration for a single CUCM server and one CUBE

CUBE needs to be configured with physical interface will be configured with a secondary IP address.

```
interface FastEthernet 0/0.<INTERFACE>

   ip address <PRIMARY_IP_ADDR> <Mask>

   ip address <SECONDARY_IP_ADDR> <Mask> secondary
```

CUCM will be configured with 2 different SIP trunks :

- 1st SIP trunk pointing to the primary address of the CUBE
- 2nd SIP trunk pointing to the secondary address of the CUBE

CUCM will be configured with a Route List composed of (at least) 2 Route Groups. Each route group will include one of the SIP trunk configured. On each route group parameters, a specific prefix should be defined. This way the CUBE will be able to route the outgoing calls to the right SBC, depending on this prefix value:

```
dial-peer voice 1 voip

   description **CUCMBE**

   answer-address 227....

   destination-pattern 227....

   session target ipv4:<CUCMBE_IP>

   […]


!For outgoing calls (with a prefix to select the target SBC)

dial-peer voice 11 voip

   description ** Outgoing calls - Outbound dial peer - SBC1 side **

   answer-address 227....

   destination-pattern 11T

   session-target <SBC1_IP>

   […]


dial-peer voice 12 voip

   description ** Outgoing calls - Outbound dial peer - SBC2 side **
   answer-address 227....

   destination-pattern 12T

   session-target <SBC2_IP>

   […]


dial-peer voice 101 voip

 description ** Incoming calls - Inbound dial peer - SBC side **

 answer-address +.T

 voice-class codec 1

 voice-class sip send 180 sdp

 session protocol sipv2

 dtmf-relay rtp-nte

no vad

!
```

9.5 Configuration for a CUCM cluster and one CUBE

CUBE needs to be configured with physical interface will be configured with a secondary IP address.

```
interface FastEthernet 0/0.<INTERFACE>

   ip address <PRIMARY_IP_ADDR> <Mask>

   ip address <SECONDARY_IP_ADDR> <Mask> secondary
```

CUCM cluster will be configured with 2 different SIP trunks :

- 1st SIP trunk pointing to the primary address of the CUBE
- 2nd SIP trunk pointing to the secondary address of the CUBE

CUCM will be configured with a Route List composed of (at least) 2 Route Groups. Each route group will include one of the SIP trunk configured. On each route group parameters, a specific prefix should be defined. This way the CUBE will be able to route the outgoing calls to the right SBC, depending on this prefix value:

For incoming and outgoing calls for CUCMs side

```
dial-peer voice 1 voip

   description **CUCM SUB**

   preference 1

   answer-address 227....

   destination-pattern 227....

   voice-class codec 1

   session target ipv4:<CUCM2_IP>

   […]


dial-peer voice 2 voip

   description **CUCM PUB**

   preference 2

   answer-address 227....

   destination-pattern 227....

   voice-class codec 1

   session target ipv4:<CUCM1_IP>
   […]
```

For outgoing calls (with a prefix to select the target SBC)

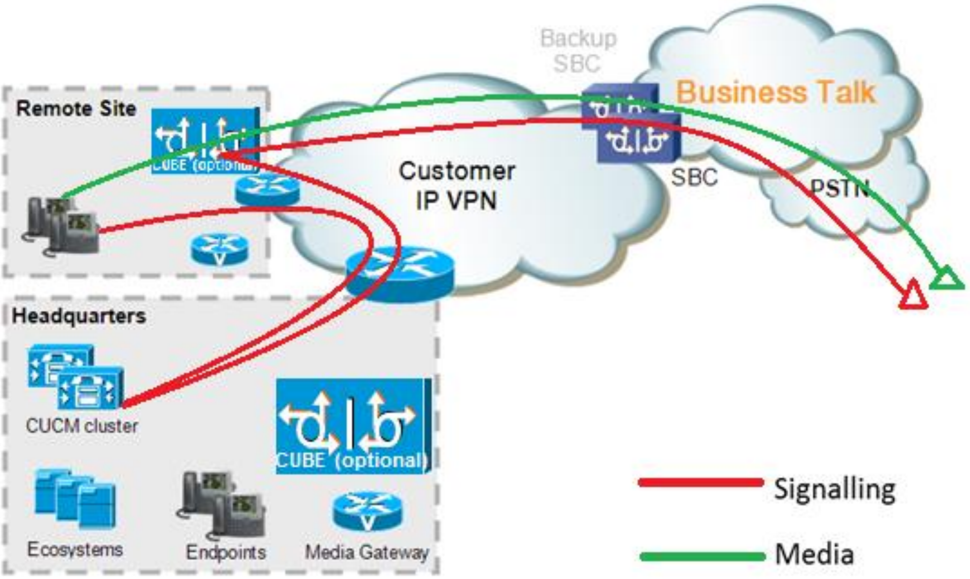
```
dial-peer voice 11 voip
   preference 1
   answer-address 227....
   destination-pattern 11T
   session-target <SBC1_IP>
   […]
dial-peer voice 12 voip
   preference 2
   answer-address 227....
   destination-pattern 12T
   session-target <SBC2_IP>
   […]
```

For incoming calls

```
dial-peer voice 101 voip
 description ** Incoming calls - Inbound dial peer - SBC side **
 answer-address +.T
 voice-class codec 1
 voice-class sip send 180 sdp
 session protocol sipv2
 dtmf-relay rtp-nte
 no vad
!
```

9.6 Design for Local SIP Trunking

For Local SIP Trunking the CUBE configuration remains mostly the same as for the regular configuration. The core differences concerning call routing are decided on CUCM level.



9.6.1 Region configuration

Regions are configured at **System** > **Region Information** > **Region.** They need to be associated with proper device pools later.

Codec preference lists can be configured at **System** > **Region Information** > **Audio Codec Preference List.** Codec Preference Lists could be assigned to Region configuration, however default option (**Use System Default**) should be set on all regions.

BT/BTIP services currently support only monocodec configuration, i.e. all customer sites need to use the same code. Only one of the 3 following codecs is supported**:**

- G.729
- G.711 A-law/u-law - CUCM doesn't allow to specify G.711 companding type (A-law or u-law), so simply choose G.711

Note that CUCM does not allow also to differentiate between G.711 and G.722 in Region settings.

Consider the following customer design:

- central site (HQ) with CUCM cluster
- a single remote site (RS) with local CUBE and call processing on HQ

Region	Purpose
HQ	Assigned to devices in the HQ site
RS	Assigned to devices in the Remote Site
WAN	Assigned to SIP trunk to BT/BTIP

Regions configuration example for customer using G.729

G.711/G.722 for intrasite calls and low-bitrate G.729 for calls over the WAN

From To	HQ	RS	WAN
HQ	**G.711/G.722**	G.729	G.729
RS	G.729	**G.711/G.722**	G.729
WAN	G.729	G.729	G.729

Regions configuration example for customer using G.711

G.711 or G.722 used for intrasite calls, for calls over the WAN - G.711.

From To	HQ	RS	WAN
HQ	G.711/G.722	G.711/G.722	G.711
RS	G.711/G.722	G.711/G.722	G.711
WAN	G.711	G.711	G.711

9.6.2 Device Pool configuration

Go to **System** > **Device Pool** and press **Add new** button.

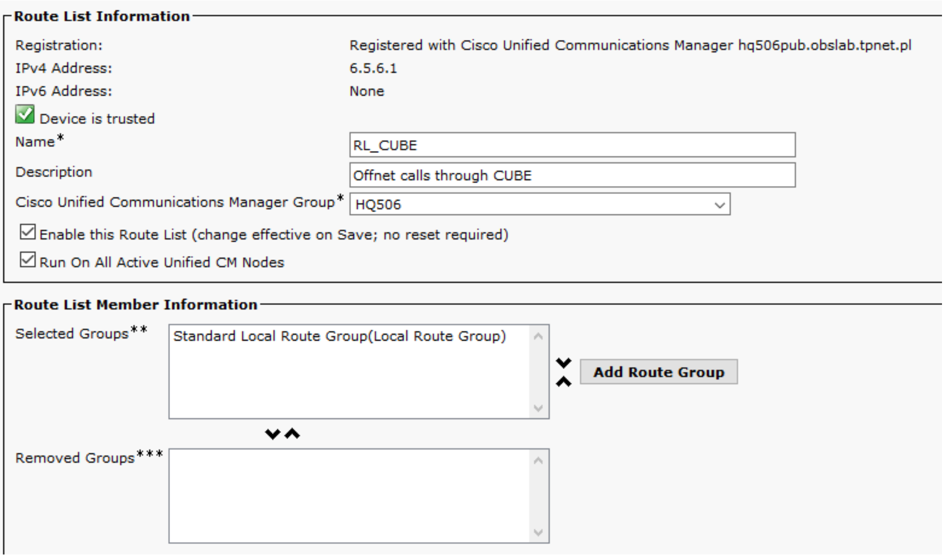
Under Device Pool configuration there are several important parameters:

- The number of Device Pools at least should be the same as the number of sites
- Every Device Pool should has appropriate Region and Location value
- Media Resource Group List need to be add with all resources (annuciator, MOH Server, transcoder, conference, software MTP). See Media Resources section- 2.5).
- **Standard Local Route Group** may be configured in order to enable routing through local CUBE without modifying CSS and partitions. Site-specific Route Group should be set as Standard Local Route Group. If Standard Local Route Group is used, then it should be configured for every device pool depending on the expected trunk to be used. **Note that the Local Route Group used is based on the call originator's device pool in case the call is forwarded.**

Note: MOH server requires a separate Device Pool configuration.

9.6.3 Route List configuration

Standard Local Route Group is configured under the **Route List** used for offnet calls



Route List Information

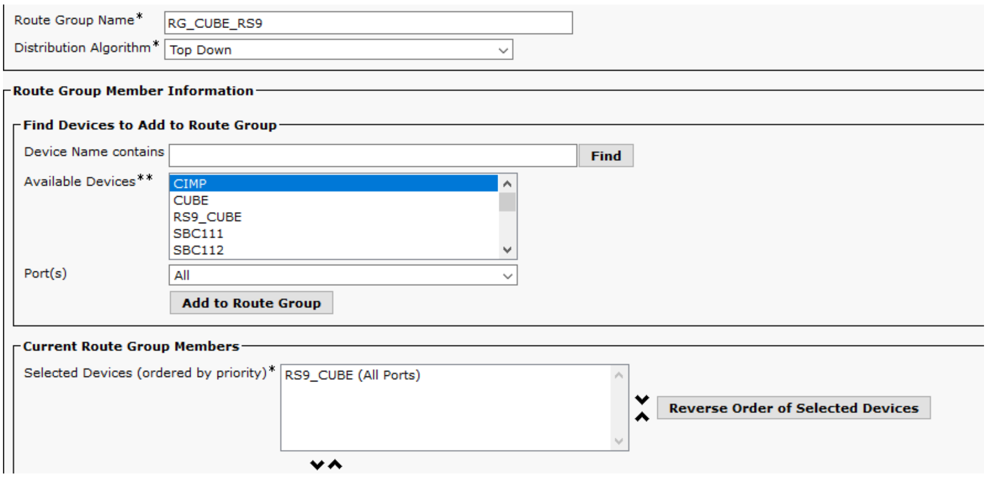
Registration: Registered with Cisco Unified Communications Manager hq506pub.obslab.tpnet.pl
IPv4 Address: 6.5.6.1
IPv6 Address: None
☑ Device is trusted
Name* RL_CUBE
Description Offnet calls through CUBE
Cisco Unified Communications Manager Group* HQ506
☑ Enable this Route List (change effective on Save; no reset required)
☑ Run On All Active Unified CM Nodes

Route List Member Information

Selected Groups** Standard Local Route Group(Local Route Group)
Removed Groups***

9.6.4 Route Group Configuration

Route Groups should be configured for each site with trunks used for Offnet calling – either via CUBE or directly towards Orange SBC.



Route Group Name* RG_CUBE_RS9
Distribution Algorithm* Top Down

Route Group Member Information

Find Devices to Add to Route Group

Device Name contains
Available Devices** CIMP, CUBE, RS9_CUBE, SBC111, SBC112
Port(s) All

Current Route Group Members

Selected Devices (ordered by priority)* RS9_CUBE (All Ports)

9.6.5 Locations (Call Admission Control)

Go to **System** > **Location Info** > **Location** and press **Add new** button.

Warning! RSVP locations are not supported!

For customers using IP VPN to connect all their locations, Static Locations CAC feature in CUCM is well-suited. In such case, **the default Hub_None location with unlimited bandwidth should be**

used to represent the IP VPN cloud (no devices should be associated with it). Each site should have a dedicated location to track bandwidth used on its WAN link.

9.6.6 SIP Trunk Configuration

The configuration of SIP Trunks remains standard. Additional SIP Trunks have to be configured toward the Local CUBE. Device Pool used for the trunks toward Local CUBE should be site-specific and contain Standard Local Route Group corresponding to that CUBE. For details on SIP Trunk configuration consult CUCM Configuration Checklist.

10 CUBE Secure configuration of SIP Trunk over Internet (BToI/BTIPoI)

Connect to the CUBE configuration CLI and enable administrative rights.

10.1 NTP server

These commands synchronize the clock of the router. Ideally, NTP requires 3 servers. Configuration adjusts the GMT time to the France time zone, taking into account the change between winter and summer and vice-versa. It should be adjusted as needed. NTP clock synchronization is necessary for correct management of certificates.

```
clock timezone GMT+1 1
clock summer-time GMT+2 recurring last Sun Mar 3:00 last Sun Oct 3:00
ntp server {IP_NTP_server}
```

10.2 Generate RSA Keypair

The below configuration is performed from global configuration level. <RSA NAME> in the command below is a label for convenience, this can be any name.

```
crypto key generate rsa general-keys label <RSA NAME> modulus 2048
```

10.3 Create Trustpoints

Trustpoints are used for SIP TLS communication and have to be created according to the internal Certificate Authority structure and certificate deployment method. Below configuration example is created for a certificate chain consisting of a Root CA certificate and Intermediate certificate and manual certificate deployment. Depending on internal security rules, deployment and revocation configuration may be different. Two trustpoints must be created – one for Root CA certificate, the other for intermediate certificate and external communication between CUBE and Orange SBC.

10.3.1 SBC Root Trustpoint

```
crypto pki trustpoint <CA ROOT TRUSTPOINT NAME>
 enrollment terminal
 revocation-check none
```

Parameter	Description
< CA ROOT TRUSTPOINT NAME>	The name of trustpoint used for SBC Root CA certificate, this is just a label for convenience

10.3.2 Intermediate Trustpoint

```
crypto pki trustpoint <CA INTERMEDIATE TRUSTPOINT NAME>
```

```
 enrollment terminal pem
 serial-number none
 ip-address none
 subject-name CN=<CUBE HOSTNAME>
 chain-validation continue <CA ROOT TRUSTPOINT NAME>
 revocation-check none
 rsakeypair <RSA NAME>
```

Parameter	Description
<CA INTERMEDIATE TRUSTPOINT NAME>	The name of trustpoint, this is just a label for convenience
<CUBE HOSTNAME>	X.509 Subject name, this value must be configured on a public DNS for CUBE to be reachable from Internet
<RSA NAME>	The name of RSA Keypair generated in previous step

10.4 Generate CUBE Certificate Signing Request (CSR)

1. The crypto pki enroll <CA INTERMEDIATE TRUSTPOINT NAME> command produces the CSR that is provided to the Enterprise CA to get the signed certificate. The output between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST (including these lines) must be copied and saved into notepad file or pasted directly into CA certificate signing submission. Below is an example of the output of this command.

```
CUBE-2(config)#crypto pki enroll SUBCA1
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=CUBE-2
% The subject name in the certificate will include: CUBE-2
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIICjjCCAXYCAQAwKDEPMA0GA1UEAxMGQ1VCRS0yMRUwEwYJKoZIhvcNAQkCFgZD
VUJFLTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDAmVvufevAg1ip
Kn8FhWjFlNNUFMqkgh2Cr1IMV+ovR2HyPTFwgr0XDhZHMSsnBw67Ttze3Ebxxoau
cBQcIASZ4hdTSIgjxG+9YQacLm9MXpfxHp5kcICzSfSllrTexArTQglW8+rErYpk
2THN1S0PC4cRlBwoUCgB/+KCDkjJkUy8eCX+Gmd+6ehRKEQ5HdFHEfUr5hc/7/pB
liHietNKSxYEOr9TVZPiRJrtpUPMRMZElRUm7GoxBrCWIXVdvEAGC0Xqd1ZVLlTz
z2sQQDqvJ9fMN6fngKv2ePr+f5qejWVzGO0DFVQs0y5x+Yl+pHbsdV1hSSnPpJk6
TaaBmX83AgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDAN
BgkqhkiG9w0BAQUFAAOCAQEArWMJbdhlU8VfaF1cMJIbr569BZT+tIjQOz3OqNGQ
QpzHwclLoaKuC5pc/u0hw14MGS6Z440Iw4zK2/5bb/KL47r8H3d7T7PYMfK6lAzK
sU9Kf96zTvHNWl9wXImB5blJfRLXnFWXNsVEF4FjU74plxJL7siaa5e86eNy9deN
20iKjvP8o4MgWewILrD01YZMDMDS1Uy82kWI6hvXG5+xBT5A1lo2xCj1S9y6/D4d
f0ilDZvaQk+7jjBCzLv5hET+1neoQBw52e7RWU8s2biQw+7TEAdO8NytF3q/mA/x
bUKw5wT4pgGUJcDAWej3ZLqP91g5yyd9MiCdCRY+3mLccQ==
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
CUBE-2(config)#
```

2. Get CUBE signed by Certificate Authority. Use CSR generated in step 1.

3. The Root certificate provided by OBS can be opened in notepad and copy-pasted into CUBE. In order to import CA Root certificate use crypto pki authenticate <CA Root Trustpoint Name> command.

```
CUBE-2(config)#
CUBE-2(config)#crypto pki authenticate ROOT

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIQMVF/OWq+ELxFC2IdUGvd2jANBgkqhkiG9w0BAQUFADBQ
MRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExIjAg
BgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEtQ0EwHhcNMTQwOTEzMjMzODA2
WhcNMTkwOTEzMjM0ODA1WjBQMRIwEAYKCZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJ
k/IsZAEZFgZzb3BoaWExIjAgBgNVBAMTGXNvcGhpYS1XSU4tM1MxOEpDM0xNMkEt
Q0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4aywr1oOpTdTrM8Ya
R3RkcahbbhR3q7P1luTDUDNM5Pi6P8z3MckfjB/yy6SWr1QnddhyvMG6IGNtVxJ4
eyw0c7jbArXWOemGLOt454A0mCfcbwMhjQBycg9SM1r1Umzad7kOCzj/rD6hMbC4
jXpg6uU8g7eB3LzN1XF93DHjxYCBKMIeG45pqmsOc3mUj1CbCtnYXgno+mfhNzhR
HSth02z4XlGm99v46j/PqGjNRq4WKCwDc45SG3QjJDqDxnRJPKtRdNva66UJfDJp
4YMXQxOSkKMtDEDhH/Eic7CrJ3EywpUpMZAmqh4bmQ7Vo2pnRTbYdaAv/+yr8sMj
+FU3AgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBTvo1P6OP4LXm9RDv5MbIMk8jnOfDAQBgkrBgEEAYI3FQEEAwIBADANBgkq
hkiG9w0BAQUFAAOCAQEAmd7hJ2EEUmuMZrc/qtSJ223loJlpKEPMVi7CrodtWSgu
5mNt1XsgxijYMqD5gJe1oq5dmv7efYvOvI2WTCXfwOBJ0on8tgLFwp1+SUJWs95m
OXTyoS9krsI2G2kQkjQWniMqPdNxpmJ3C4WvQLPLwtEOSRZRBvsKy6lczrgrV2mZ
kx12n5YGrGcXSblPPUddlJep1l8U+AQC8wkSzfJu0yHJwoH+lrIfgqKUee4x7z6s
SCaGddCYr3OK/3Wzs/WjSO2UETvNL3NEtWHDc2t4Y7mmIMSDvGjHZUgGZotwc9kt
9f2dZA0rtgBq4IDtpxkR3CQaauB7wUCpzemHzf+z9Q==
-----END CERTIFICATE-----

Certificate has the following attributes:
 Fingerprint MD5: 511E1008 6D315E03 4B748601 7EE1A0E5
 Fingerprint SHA1: 8C35D9FA 8F7A00AC 0AA2FCA8 AAC22D5F D08790BB

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

CUBE-2(config)#
```

4. Using the same procedure as in the previous step, import the intermediate SBC certificate provided by OBS using crypto pki authenticate <CA Intermediate Trustpoint Name>.

5. Import CA signed Certificate. The signed certificate provided by CA can be opened in notepad and copy-pasted into CUBE. To import certificate use crypto pki import <CA Intermediate Trustpoint Name> certificate command. Below is an example of this command:

```
CUBE-2(config)#crypto pki import SUBCA1 certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIEAjCCAuqgAwIBAgIKQZZrHQABAAAAEzANBgkqhkiG9w0BAQUFADBJMRIwEAYK
CZImiZPyLGQBGRYCbGkxFjAUBgoJkiaJk/IsZAEZFgZzb3BoaWExGzAZBgNVBAMT
```

```
EnNvcGhpYS1FWENIMjAxMC1DQTAeFw0xNTA0MDEwMDEzNDFaFw0xNjA0MDEwMDIz
NDFaMBExDzANBgNVBAMTBkNVQkUtMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAMCZW+5968CDWKkqfwWFaMWU01QUyqSCHYKvUgxX6i9HYfI9MXCCvRcO
FkcxKycHDrtO3N7cRvHGhq5wFBwgBJniF1NIiCPEb71hBpwub0xel/EenmRwgLNJ
9KWWtN7ECtNCCVbz6sStimTZMc3VLQ8LhxGUHChQKAH/4oIOSMmRTLx4Jf4aZ37p
6FEoRDkd0UcR9SvmFz/v+kGWIeJ600pLFgQ6v1NVk+JEmu2lQ8xExkSVFSbsajEG
sJYhdV28QAYLRep3VlUuVPPPaxBAOq8n18w3p+eAq/Z4+v5/mp6NZXMY7QMVVCzT
LnH5iX6kdux1XWFJKc+kmTpNpoGZfzcCAwEAAaOCASIwggEeMA4GA1UdDwEB/wQE
AwIFoDAdBgNVHQ4EFgQU9PbHMHSkYrjJ2+/+hSSMEoma0QIwHwYDVR0jBBgwFoAU
rHWCWSFPSF8hpvWi+u/vLg4TPxMwTwYDVR0fBEgwRjBEoEKgQIY+ZmlsZTovL0VY
Q0gyMDEwLnNvcGhpYS5saS9DZXJ0RW5yb2xsL3NvcGhpYS1FWENIMjAxMC1DQSgx
KS5jcmwwbQYIKwYBBQUHAQEEYTBfMF0GCCsGAQUFBzAChlFmaWxlOi8vRVhDSDIw
MTAuc29waGlhLmxpL0NlcnRFbnJvbGwvRVhDSDIwMTAuc29waGlhLmxpX3NvcGhp
YS1FWENIMjAxMC1DQSgxKS5jcnQwDAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQUF
AAOCAQEAe7EAoXKIAij4vxZuxROOFOfsmjcojU31ac5nrLCbq/FyW7eNblphL0NI
Dt/DlfZ5WK2q3Di+/UL1lDt3KYt9NZ1dLpmccnipbbNZ5LXLoHDkLNqt3qtLfKjv
J6GnnWCxLM18lxm1DzZT8VQtiQk5XZ8SC78hbTFtPxGZvfX70v22hekkOL1Dqw4h
/3mtaqxfnslB/J3Fgps1och45BndGiMAWavzRjjOKQaVLgVRvVrPIy3ZKDBaUleR
gsy5uODVSrhwMo3z84r+f03k4QarecgwZE+KfXoTpTAfhiCbLKw0ZyRMXXzWqNfl
iotEQbs52neCwXNwV24aOCChQMw2xw==
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

10.5 Assign Trustpoint for sip-ua

This configuration has to be done for all CUCM nodes. The configuration can be done on IP address basis, or a default trustpoint can be configured for all sip signaling from CUBE.

```
sip-ua
 crypto signaling default trustpoint <CA Intermediate Trustpoint name>
```

10.6 SIP Trunk over Internet media source ports configuration

“Voice service voip” allows for RTP port range hardening for transmitting media over UDP.

The Orange **BTIP** SIP Trunk service specifies that customers uses RTP ports in the range of **6000 – 20000.**The Orange **BT** SIP Trunk service specifies that customers uses RTP ports in the range of **6000 – 38000**. However **CUBE media source ports** can be configured within a range of **8000-48198.**

Configuration of media source ports on CUBE for **BTIPoI:**

```
!

voice service voip

 rtp-port range 8000 20000

!
```

Configuration of media source ports on CUBE for **BToI:**

```
!
voice service voip
 rtp-port range 8000 32000
!
```

10.7 SIP Trunk over Internet configuration example

> **Note**: This chapter focuses on BToI/BTIPoI SIP trunk configuration on CUBE indicating the required update of configuration in addition to already implemented BT/BTIP configuration described in previous chapters.

The Cisco Unified Border Element (CUBE) deployment enables TLS encryption of the signaling traffic and SRTP encryption of the media traffic carried over public internet between CUBE and Orange A-SBC.

Public key certificate is used to identify the CUBE when performing a TLS handshake for incoming and outgoing connections over Internet.

> **Note**: Media must be terminated on CUBE to perform media transcoding between internal **RTP** and external **SRTP**. Media flow through must be enabled.

SIP Trunk over Internet configuration example:

```
dial-peer voice 11 voip
 description *** Nominal SIP Trunk over Internet SBC ***
 preference 1
 answer-address 227....
 destination-pattern 11T
 session protocol sipv2
 session target dns:<Nominal_FQDN_Orange_SBC1>
 session transport tcp tls
 srtp
[...]
dial-peer voice 12 voip
 description *** Backup SIP Trunk over Internet SBC ***
 preference 2

 answer-address 227....

 destination-pattern 12T

 session protocol sipv2

 session target dns:<Backup_FQDN_Orange_SBC2>

 session transport tcp tls

 srtp

[...]
```

11 CUCM with Oracle Session Border Controller configuration

11.1 CUCM configuration

Below is the configuration required on the CUCM side to setup SIP trunk to Oracle SBC. Please note that if some of this configuration has been previously done – for example SIP Profile, it can be reused and there is no need to create separate objects.

Off-net calling via BT/BTIP Diversion Header manipulation Partition	
Menu	**Value**
Call Routing -> Class of Control -> Partition -> Add new	
Name	DIV-HEADER-PT
Off-net calling via BT/BTIP Diversion Header manipulation Called Party Transformation Pattern	
Call Routing -> Transformation -> Transformation Pattern -> Called PartyTransformation Pattern -> Add New	
Pattern	XXXX
Prefix digits	Site Prefix
Off-net calling via BT/BTIP Diversion Header manipulation Calling Search Space	
Call Routing -> Class of Control -> Calling Search Space -> Add New	
Name	DIV-HEADER-CSS
Selected Partitions	DIV-HEADER-PT
Off-net calling via BT/BTIP Basic Configuration Sip Trunk Security Profile	
System > Security > SIP Trunk Security Profile, select “Non Secure SIP Trunk Profile” from SIP Trunk Security Profile List	
Incoming Transport Type	TCP + UDP
Outgoing Transport Type	UDP
Off-net calling via BT/BTIP Basic Configuration SIP Profile	
Device > Device Settings > SIP Profile	
User-Agent and Server header information	Send Unified CM Version Information as User-Agent Header
Version in User Agent and Server Header	Full Build
SIP Rel1XX Options	Send PRACK for 1xx Messages
Early Offer support for voice and video	Mandatory (insert MTP if needed)
Send send-receive SDP in mid-call INVITE	Checked

Ping Interval for In-service and Partially In-service Trunks (seconds)	300
Ping Interval for Out-of-service Trunks (seconds)	5
Version in User Agent and Sever Header	Full build
Session Refresh Method	INVITE or UPDATE

Version in User Agent and Sever Header - inject info about full version of CUCM
Session Refresh Method - since CUCM 10.0 there is additional method – “UPDATE”. “INVITE” should be used by default.

Off-net calling via BT/BTIP

Basic Configuration

SIP Normalization Script

Device > Device Settings > SIP normalization script > Add new

SIP Normalization Script is applied to SIP trunk and is required to adapt the SIP signaling to the form expected by BT/BTIP infrastructure.
The content of the script is given below:

```
-- Orange SIP Normalization Script v11
-- this is normalization script for uc 12.x or later
M = {}


-- This is called when an INVITE message is sent
function M.outbound_INVITE(msg)
    local sdp = msg:getSdp()
    if sdp
    then
       -- remove b=TIAS:
       sdp = sdp:gsub("b=TIAS:%d*\r\n", "")
       -- store the updated sdp in the message object
       msg:setSdp(sdp)
    end
end


--modifying of Server header in 183 messages
function M.outbound_183_INVITE(msg)
-- change 183 to 180 if sdp
 local sdp = msg:getSdp()
 if sdp
 then
  msg:setResponseCode(180, "Ringing")
 end
end

--modifying of Server header in 488 messages
function M.outbound_488_INVITE(msg)
 -- change 488 to 503 if sdp
```

```
  msg:setResponseCode(503, "Service Unavailable")
end

--handling of 400 errors
function M.inbound_400_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
  msg:addHeader("Reason", "Q.850; cause=27")
 end
end

--handling of 403 errors
function M.inbound_403_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 408 errors
function M.inbound_408_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 480 errors
function M.inbound_480_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=20")
 end
end

--handling of 481 errors
function M.inbound_481_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=27")
 else
  msg:addHeader("Reason", "Q.850; cause=27")
 end
end

--handling of 487 errors
function M.inbound_487_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=16")
 end
end

--handling of 488 errors
function M.inbound_488_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if not reason
 then
  msg:addHeader("Reason", "Q.850; cause=127")
 end
end

--handling of 500 errors
function M.inbound_500_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 501 errors
function M.inbound_501_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=2")
 else
  msg:addHeader("Reason", "Q.850; cause=2")
 end
end

--handling of 502 errors
function M.inbound_502_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:removeHeader("Reason")
 end
end

-- handling of 503 errors
function M.inbound_503_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 505 errors
function M.inbound_505_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- handling of 513 errors
function M.inbound_513_INVITE(msg)
 local reason = msg:getHeader("Reason")
 if reason
 then
  msg:modifyHeader("Reason", "Q.850; cause=38")
 else
  msg:addHeader("Reason", "Q.850; cause=38")
 end
end

-- addition of PAI header if incoming INVITE includes Privacy
header
function M.inbound_INVITE(msg)
 -- get Privacy header
 local privacy = msg:getHeader("Privacy")
 if privacy
 then
  -- get From and Pai
  from = msg:getHeader("From")
  pai = msg:getHeader("P-Asserted-Identity")
  --check if Pai header is not present
  if pai==nil
  then
   -- add Pai header filled with From URI value
   local uri = string.match(from, "(<.+>)")
   msg:addHeader("P-Asserted-Identity", uri)
  end
 end
end

return M
```

Off-net calling via BT/BTIP Basic Configuration SIP Trunk Configuration	
Menu	**Value**
Device > Trunk > Add new	
Device Pool	Choose Device Pool which include Region and Location value
Media Resource Group List	MRGL
Redirecting Diversion Header Delivery - Inbound	Checked
Redirecting Diversion Header Delivery - outbound	Checked
Destination Address	Oracle SBC IP Address
SIP Trunk Security Profile	SIP Trunk Security Profile name
SIP Profile	Standard SIP Profile with PRACKs, EO, Send-recv

DTMF Signaling Method	RFC 2833
Normalization Script	SIP Normalization Script name (currently v11)
Enable Trace	Unchecked
Redirecting Party Transformation CSS	DIV-HEADER-CSS
Media Termination Point Required	**Checked**
Off-net calling via BT/BTIP **Basic Configuration** **Route Group**	
Call Routing > Route/Hunt > Route group > Add new	
Distribution algorithm	Top Down
Selected devices	SIP trunk to ORACLE SBC
Off-net calling via BT/BTIP **Basic Configuration** **Route List**	
Call Routing > Route/Hunt > Route list > Add new	
Selected Groups	Route Group with SIP trunk to Oracle SBC
Off-net calling via BT/BTIP **Basic Configuration** **Route Pattern**	
Call Routing > Route/Hunt > Route Pattern > Add new	
Route Pattern	Specific Route Pattern
Gateway/Route List	Route List name
Call Classification	OffNet
Discard Digits	PreDot Trailing#

11.2 Oracle SBC configuration

For detailed information regarding Oracle ESBC configuration, please refer to Annex A and dedicated VISIT SIP Configuration Guideline for Oracle ESBC 8.2.

11.2.1 Oracle SBC information required for CUCM interconnection

The pieces of information needed to create a new customer on the SBC are the following ones:

Customer related data		
Code	Content	Example
<VENDOR_IPBX>	Unique identifier of the CISCO CUCM IPBX in the SBC. This field must follow 7 alphabetical characters format.	CISCO
<VLAN_ID>	It corresponds to the VLAN tag allocated to the customer. This field must follow 3 digits format.	110
NOMINAL SBC related data		
<ESBC_SOUTH_NOMINAL_GW>	IP address of the gateway in front of the nominal SBC (PE router) on access side.	138.132.169.1
<ESBC_SOUTH_NOMINAL_IP>	IP address of the nominal SBC South Side on the interconnection network.	138.132.169.2

	Cisco IPBXs will send/receive their signaling and media traffic to/from this IP address (on default port 5060 for signaling). This SBC IP address is located in /29 network provided by the customer. It is used to interconnect the nominal SBC on the customer private network.	
BACKUP SBC related data		
<ESBC_SOUTH_BACKUP_GW>	IP address of the gateway in front of the backup SBC (PE router) on access side.	138.132.179.1
<ESBC_SOUTH_BACKUP_IP>	IP address of the backup SBC SBC South Side on the interconnection network. Cisco IPBXs will send/receive their signaling and media traffic to/from this IP address (on default port 5060 for signaling). This SBC IP address is located in /29 network provided by the customer. It is used to interconnect the backup SBC on the customer private network.	138.132.179.2

11.2.2 Oracle SBC information required for a new IPBX

This chapter specifies which IP addresses need to be indicated in the session agents and the distribution of the session agents in the session agent groups.
The information indicated in the document will help you to fill in the table here after.

The pieces of information needed to create a new IPBX on the e SBC are the following ones:

IPBX related data		
Code	Content	Example
<PBX type>	PBX type, version and configuration. Information needed to define which SA and SAG need to be created, and if specific profile is required.	Cisco CUCM 12.0
<SIP_PROFILE>	This identifier is used to differentiate several SIP profiles. It depends on the type of IPBX (Vendor & version). Specific SBC configuration is linked to each profile, each one corresponding to a Prod+ template. The profile follows 2 digits format. Values: 00: Default profile is number 00 05: Cisco CUCM	05
<Number of Elements for nominal IPBX>	Number of signaling entities to be declared as SA and included in the nominal SAG.	2
<Number of Elements for backup IPBX>.	Number of signaling entities to be declared as SA and included in the backup SAG.	2
<IPBX_NOMINAL_SA1_IP> to <IPBX_NOMINAL_SAn_IP>	IP addresses of the IPBX signaling entities. These entities belong to nominal session agent group.	6.5.6.1 6.5.6.2
<IPBX_BACKUP_SA1_IP> to <IPBX_BACKUP_SAn_IP>	IP addresses of the IPBX signaling entities. These entities belong to backup session agent group.	6.5.6.1 6.5.6.2
<SA_X>	It is a 2 digits number representing the element number within the nominal IPBX. X is varying from 1 to < Number of Elements for nominal IPBX>	01
<SA_Y>	It is a 2 digits number representing the element number within the backup IPBX. Y is varying from 1 to < Number of Elements for backup IPBX>.	01

11.2.3 Information required for BTIP / Btalk SIP Infrastructure

This chapter specifies which IP addresses need to be indicated in the session agents and the distribution of the session agents in the session agent groups.
The information indicated in the document will help you to fill in the table here after.

The pieces of information needed to create a new IPBX on the e SBC are the following ones:

IPBX related data		
Code	Content	Example
<BT_NOMINAL_SA_IP>	IP addresses of the BT/BTIP signaling entities. These entities belong to nominal session agent group.	172.22.246.33 X.X.X.X.
<BT_BACKUP_SA_IP>	IP addresses of the BT/BTIP signaling entities. These entities belong to backup session agent group.	172.22.246.73 X.X.X.X
<SA_X>	It is a 2 digits number representing the element number within the nominal C-SBC. X is varying from 1 to < Number of Elements for nominal ESBC>	01
<SA_Y>	It is a 2 digits number representing the element number within the backup C-SBC. Y is varying from 1 to < Number of Elements for backup ESBC>.	01

11.2.4 SBC Object naming convention

Based on previous information, the following table presents identifiers that will be created in SBC configuration. These unique identifiers are mandatory to configure the SBC. The rules presented below are valid for both Nominal and Backup A-SBC.

SBC OBJECTS	
Name	Description
Customer identifier	Unique identifier of the customer within the SBC on the access part. It is used to configure the name of the access parent realm. Rule is: ACC_<VLAN_ID>_<IPBX_VENDOR>
Nominal IPBX identifier	Unique identifier of the Nominal IPBX within the SBC. It is used to configure the nominal Session-Agent-Group. It is proposed to used the SIP profile, VLAN Id and the T1T7 parameters to configure it. Rule is: N_<VLAN_ID>_<IPBX_VENDOR>_SIP_PROFILE>
Backup IPBX identifier	Unique identifier of the Backup IPBX within the SBC. It is used to configure the backup Session-Agent-Group. It is proposed to used the SIP profile, VLAN Id and the T1T7 parameters to configure it. Rule is: B_<VLAN_ID>_<IPBX_VENDOR>_<SIP_PROFILE>
Element [X] identifier for the Nominal IPBX	Unique identifier of the Element X of the Nominal IPBX within SBC. It is used to configure the nominal Session-Agent that will be included in the nominal Session-Agent-Group. It is proposed to used the VLAN Id and the T1T7 parameters to configure it. Rule is: N-<VLAN_ID>-<IPBX_VENDOR>-<SA_X> Note that underscores are not allowed in hostnames of Session-Agents. Hence, hyphens are used instead.
Element [Y] identifier for the Backup IPBX	Unique identifier of the Element Y of the Backup IPBX within SBC. It is used to configure the backup Session-Agent that will be included in the backup Session-Agent-Group. It is proposed to used the VLAN Id and the T1T7 parameters to configure it. Rule is: B-<VLAN_ID>-<IPBX_VENDOR>-<SA_Y>

Maximum size of any identifier is not larger than 24.

11.2.5 Certificate

In “TLS/ Secured SIP Trunking” context, following requirements regarding Certificate configuration:

- Certificate of the certification authority (CA), signing the ESBC certificate(format X.509 Base64)
- 1 cyphered file containing both the private key and the public certificate per domain used on the ESBC, signed by a public trusted Certificate Authority to be known, aka such as Digicert CA which Orange has chosen as CA provider
- Certificate of the trusted certificate authority, and of each sub-authority having signed the above certificate (format X.509 Base64)

11.2.6 Licenses & ESBC entitlement setup

Configuration which will enable the support of the new license model based on provisioned entitlements are not covered in this configuration Guideline such as :

- adding session capacity (based on purchased capacity)
- adding new features (based on purchased license as well). Typically the case for enabling SRTP session.

12 Expressway

12.1 Architecture overview

Server components description

- Expressway Control server (Expressway C): This server is deployed on the same Datacenter LAN than UC applications inside the datacenter. The Expressway C is a SIP proxy and communication Gateway for CUCM.

- Expressway Edge server (Expressway E): This server is deployed on a DMZ inside the datacenter. The Expressway E is a SIP Proxy for devices which are located outside the internal network.

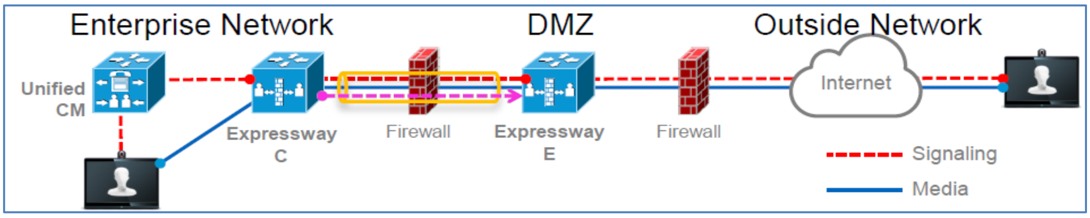
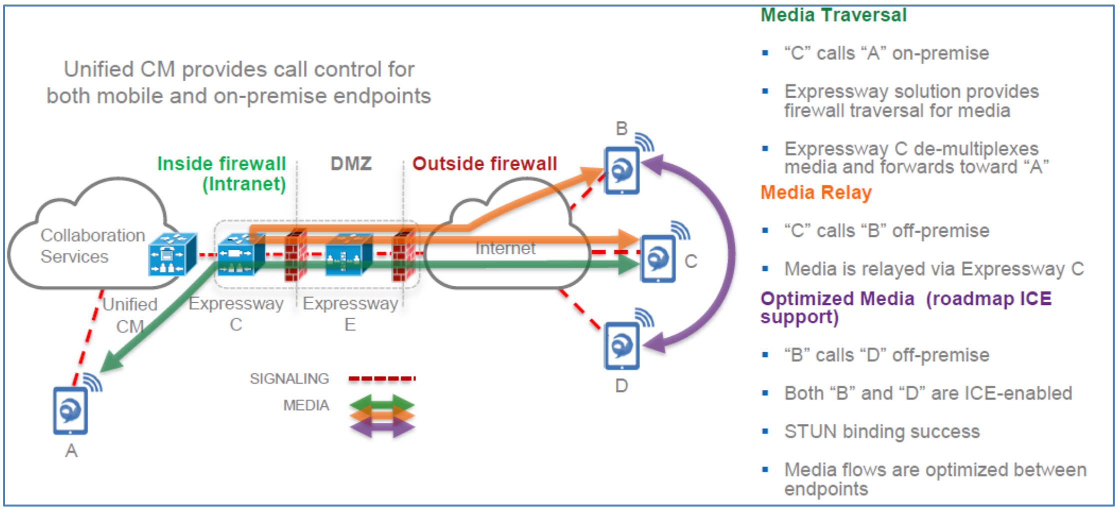


Figure Erreur ! Il n'y a pas de texte répondant à ce style dans ce document.-1 – Expressway Firewall Traversal Basics

1. Expressway E is the traversal server installed in DMZ. Expressway C is the traversal client installed inside the enterprise network.
2. Expressway C initiates traversal connections outbound through the firewall to specific ports on Expressway E with secure login credentials.
3. Once the connection has been established, Expressway C sends keep-alive packets to Expressway E to maintain the connection.
4. When Expressway E receives an incoming call, it issues an incoming call request to Expressway C.
5. Expressway C then routes the call to Unified CM to reach the called user or endpoint.
6. The call is established and media traverses the firewall securely over an existing traversal connection.

12.2 Call Flows

All mobile traffic from the internet is seen with the private Expressway-C IP address on the Customer Network.
All Mobile traffic from the customer network will be seen with the Expressway-E public IP address on the Internet.
The couple Expressway-C and Expressway-E can be seen as a proxy for call flows.
Within VISIT scope, the traffic from the internet would pass through Expressway-C and Expressway-E, through customer managed Call Manager cluster and routed further towards SIP trunk to BT/BTIP infrastructure.



Unified CM provides call control for both mobile and on-premise endpoints

Media Traversal

- “C” calls “A” on-premise
- Expressway solution provides firewall traversal for media
- Expressway C de-multiplexes media and forwards toward “A”

Media Relay

- “C” calls “B” off-premise
- Media is relayed via Expressway C

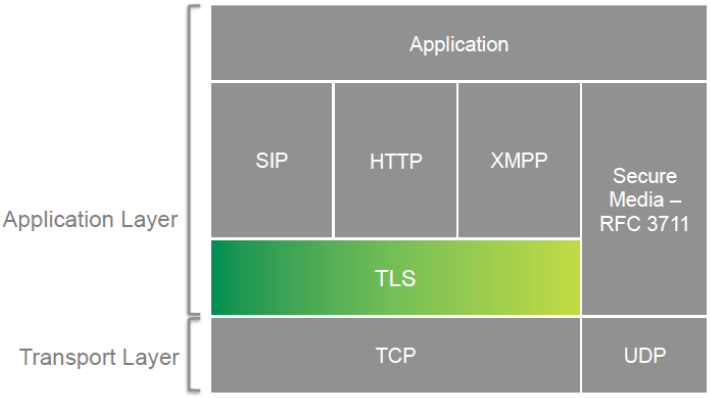
Optimized Media (roadmap ICE support)

- “B” calls “D” off-premise
- Both “B” and “D” are ICE-enabled
- STUN binding success
- Media flows are optimized between endpoints

12.3 Endpoint Authentication & Encryption

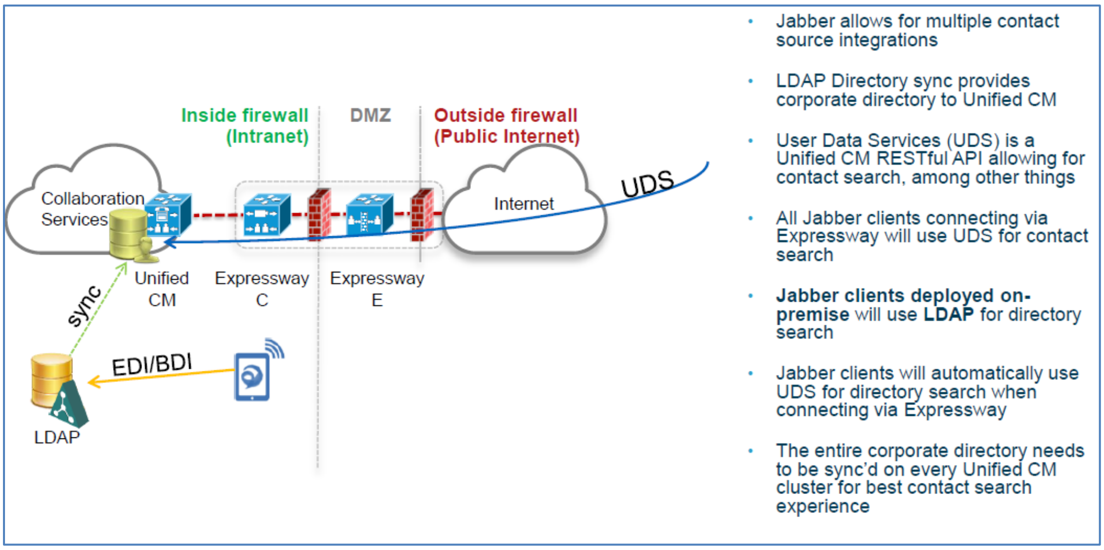
12.3.1 Authentication

Expressway use TLS which is a protocol on top of TCP layer:



12.3.2 Directory integration

Remote Jabber clients will have access to directory look-up services. Cisco Expressway uses the UDS integration model. UDS model relies on the CUCM database for directory search and phone number lookup



- Jabber allows for multiple contact source integrations
- LDAP Directory sync provides corporate directory to Unified CM
- User Data Services (UDS) is a Unified CM RESTful API allowing for contact search, among other things
- All Jabber clients connecting via Expressway will use UDS for contact search
- **Jabber clients deployed on-premise** will use **LDAP** for directory search
- Jabber clients will automatically use UDS for directory search when connecting via Expressway
- The entire corporate directory needs to be sync'd on every Unified CM cluster for best contact search experience

12.3.3 Telephony features

Cisco Jabber endpoints can be deployed using a model in which Cisco Unified Presence and Cisco Unified Communications Manager provide client configuration, instant messaging and presence, user and device management while Microsoft Active Directory provides user lookup/directory search services.

NOTE: Within VISIT scope, all currently supported features continue to function with Expressway infrastructure deployed.

Restriction: An issue has been identified that causes Jabber users registered through Expressway to not fall back to backup server in case nominal server is down.

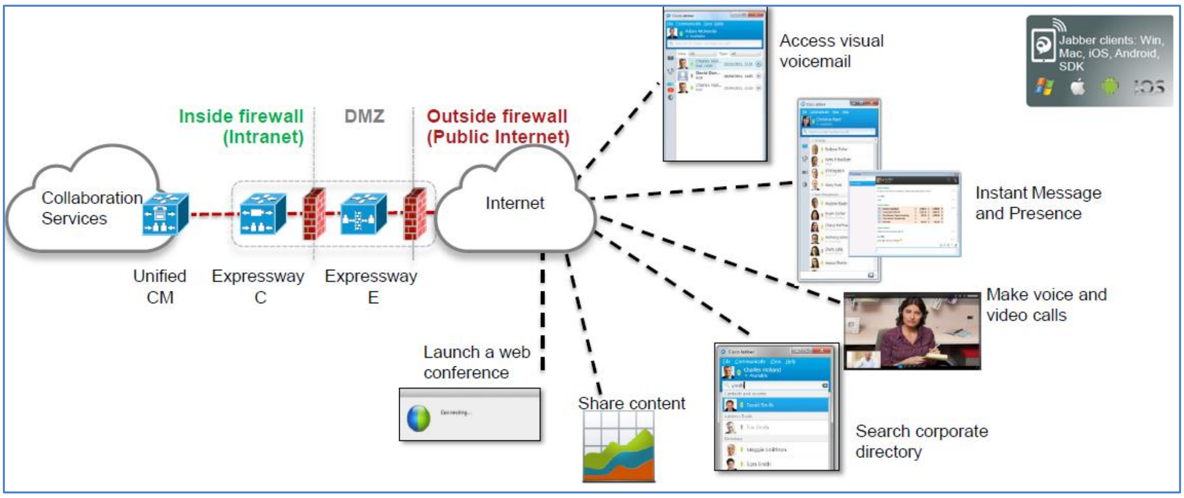
12.4 CUCM configuration update

Mobile and remote access provided by Expressway is, for most part, transparent to Cisco Unified Communications Manager. There is:

- No requirement to build a SIP trunk on CUCM to Expressway C or E,
- No requirement to make dial plan changes ,
- No remote access policy mechanism to limit edge access to certain Jabber users or devices.

Remote Jabber clients or Tele-Presence Endpoints registering to CUCM through Expressway will appear to CUCM as Expressway C IP address (opportunity for CUCM Device Mobility feature usage).

12.5 Expressway specific configuration



This solution allows Jabber clients to securely traverse the enterprise firewall and access collaboration services deployed on the enterprise network. Remote Jabber clients will have access to voice/video, instant messaging and presence, visual voicemail, and directory look-up services.

This section describes the configuration steps required on the Expressway-C.

Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

1. Ensure that System host name and Domain name are specified (System > DNS).
2. Ensure that local DNS servers are specified (System > DNS).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (System > Time). Use an Authentication method in accordance with your local policy.

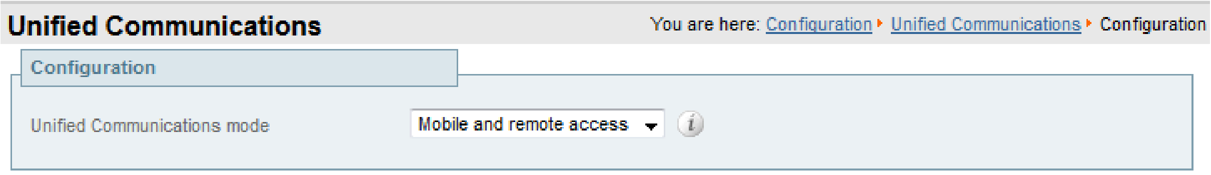
If you have a cluster of Expressways you must do this for every peer.

Configuring the Expressway-C for Unified Communications

To enable mobile and remote access functionality:

1. Go to Configuration > Unified Communications > Configuration.

2. Set Unified Communications mode to Mobile and remote access.
3. Click Save.



Unified Communications

You are here: Configuration ▸ Unified Communications ▸ Configuration

Configuration

Unified Communications mode: Mobile and remote access

Mobile and Remote Access

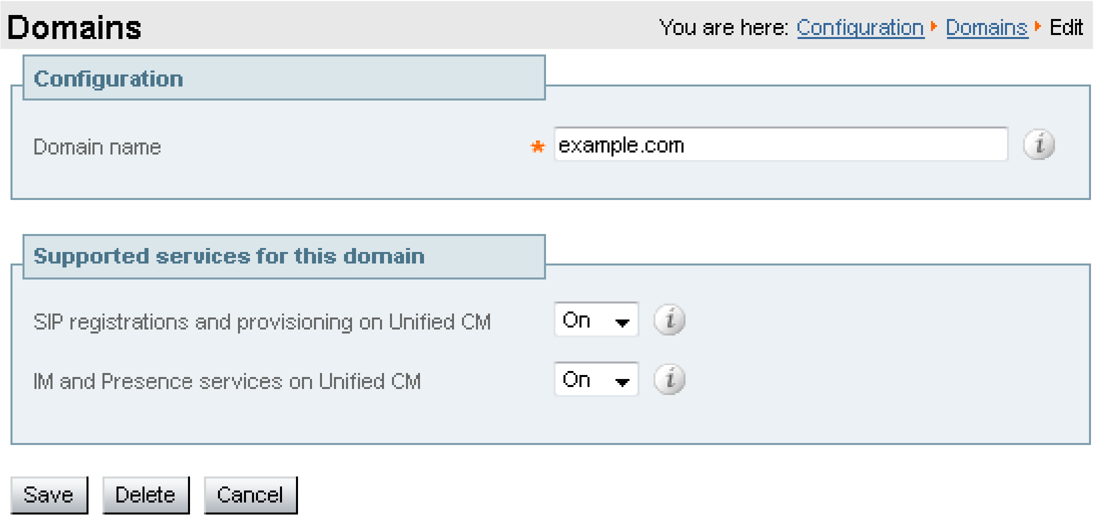
Note that you must select *Mobile and remote access* before you can configure the relevant domains and traversal zones.

Configuring the domains to route to Unified CM

You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

1. On Expressway-C, go to Configuration > Domains.
2. Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
3. For each domain, turn On the services for that domain that Expressway is to support. The available services are:
   - SIP registrations and provisioning on Unified CM: endpoint registration, call control and provisioning for this SIP domain is serviced by Unified CM. The Expressway acts as a Unified Communications gateway to provide secure firewall traversal and line-side support for Unified CM registrations.
   - IM and Presence services on Unified CM: instant messaging and presence services for this SIP domain are provided by the Unified CM IM and Presence service.

Turn On all of the applicable services for each domain.



Domains

You are here: Configuration ▸ Domains ▸ Edit

Configuration

Domain name *: example.com

Supported services for this domain

SIP registrations and provisioning on Unified CM: On

IM and Presence services on Unified CM: On

Discovering IM&P and Unified CM servers

The Expressway-C must be configured with the address details of the IM&P servers and Unified CM servers that are to provide registration, call control, provisioning, messaging and presence services. Note that IM&P server configuration is not required in the hybrid deployment model.

Uploading the IM&P / Unified CM tomcat certificate to the Expressway-C trusted CA list

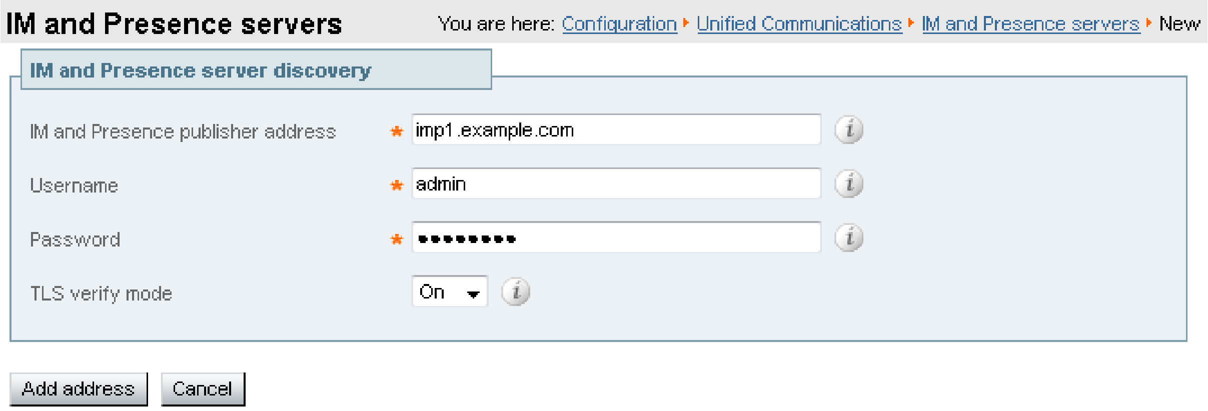
If you intend to have **TLS verify mode** set to *On* (the default and recommended setting) when discovering the IM&P and Unified CM servers, the Expressway-C must be configured to trust the tomcat certificate presented by those IM&P and Unified CM servers.

1. Determine the relevant CA certificates to upload:
   - If the servers are using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate from every IM&P / Unified CM server.
   - If the servers are using CA-signed certificates, the Expressway-C's trusted CA list must include the root CA of the issuer of the tomcat certificates.
2. Upload the trusted Certificate Authority (CA) certificates to the Expressway-C (Maintenance > Security certificates > Trusted CA certificate).
3. Restart the Expressway-C for the new trusted CA certificates to take effect (Maintenance > Restart options).

Configuring IM&P servers

To configure the IM&P servers used for remote access:

1. On Expressway-C, go to Configuration > Unified Communications > IM and Presence servers. The resulting page displays any existing servers that have been configured.
2. Add the details of an IM&P publisher:
   a. Click New.
   b. Enter the IM and Presence publisher address and the Username and Password credentials required to access the server. The address can be specified as an FQDN or as an IP address; we recommend using FQDNs when TLS verify mode is On.
   Note that these credentials are stored permanently in the Expressway database. The IM&P user must have the Standard AXL API Access role.
   c. We recommend leaving TLS verify mode set to On to ensure Expressway verifies the tomcat certificate presented by the IM&P server for XMPP-related communications.
      - If the IM&P server is using self-signed certificates, the Expressway-C's trusted CA list must include a copy of the tomcat certificate from every IM&P server.
      - If the IM&P server is using CA-signed certificates, the Expressway-C's trusted CA list must include the root CA of the issuer of the tomcat certificate.
   d. Click Add address.
   The system then attempts to contact the publisher and retrieve details of its associated nodes.



IM and Presence servers

You are here: Configuration ▸ Unified Communications ▸ IM and Presence servers ▸ New

IM and Presence server discovery

IM and Presence publisher address *	imp1.example.com
Username *	admin
Password *	•••••••••
TLS verify mode	On

IM&P Servers

Note that the status of the IM&P server will show as Inactive until a valid traversal zone connection between the Expressway-C and the Expressway-E has been established (this is configured later in this process).

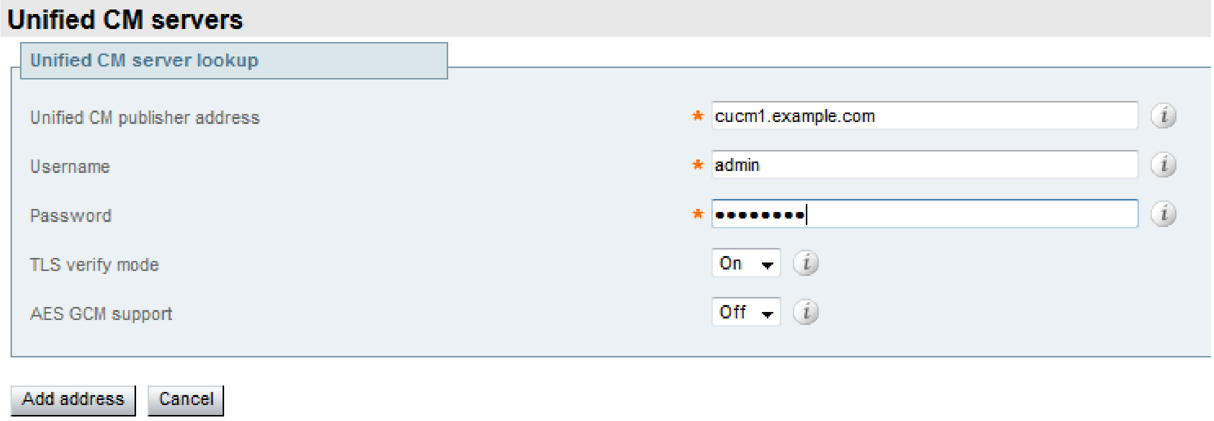
3. Repeat for every IM&P cluster.

After configuring multiple publisher addresses, you can click Refresh servers to refresh the details of the nodes associated with selected addresses.

Configuring Unified CM servers

To configure the Unified CM servers used for remote access:

1. On Expressway-C, go to Configuration > Unified Communications > Unified CM servers. The resulting page displays any existing servers that have been configured.
2. Add the details of a Unified CM publisher:



Unified CM servers

Unified CM server lookup

Unified CM publisher address *	cucm1.example.com
Username *	admin
Password *	•••••••••
TLS verify mode	On
AES GCM support	Off

13 Fax

13.1 Configuration for BT/BTIP SIP trunking

The following guide is an addition to standard SIP Trunk configuration between CUCM and VG. For more details about configuration details and steps to be done on CUCM please refer to following document:

- BTIP/BT SIP System Release 14.0 and 15.0 (IOS Voice Gateway Configuration Guide).

13.1.1 T.38 global settings

Below configuration commands are issued under voice gateway's **fax** subcommand menu.

```
voice service voip
   fax
       fax protocol t38 ls-redundancy 4 hs-redundancy 1 fallback none
```

Command	Explanation
fax protocol *protocol* ls-redundancy *value* hs-redundancy *value* fallback *type*	Choice of global fax protocol with assingment of proprer redundacy values and fallbak type

13.1.2 Codec configuration

Below configuration commands are issued under voice gateway's **voice class codec** ***tag*** subcommand menu.

```
voice class codec 1
   codec preference 1 g711alaw
   codec preference 2 g729r8
   codec preference 3 g711ulaw
```

Command	Explanation
codec preference *number codec*	*number* sets priority order (1 = Highest) *codec* sets specific codec format

13.1.3 Example of VoIP dial-peer configuration

Below configuration commands are issued under voice gateway's **dial-peer voice** subcommand menu.

```
dial-peer voice 1 voip
 preference 1
 destination-pattern .T
 session protocol sipv2
 session target ipv4:6.3.9.1
 incoming called-number .
 voice-class codec 1
 dtmf-relay rtp-nte
 fax-relay sg3-to-g3
 fax rate 14400 bytes 72
 fax nsf 000000
```

Command	Explanation
fax-relay *type*	Choice of preffered SG3 to G3 fallback method (CM blocking in TDM to IP direction)
fax rate *speed* bytes *payload*	Specifies desired speed of fax page transmission and payload
fax nsf *000000*	Specifies the fax not to use "non standard facilities"

13.1.4 POTS dial-peer

Below configuration commands are issued under voice gateway's **dial-peer voice** subcommand menu.

```
dial-peer voice 102 pots
   description fax
   destination-pattern 39001
   progress_ind alert strip
   port 0/0/0
   forward-digits all
```

Command	Explanation
description *description*	Adds a description to the dial peer.
destination-pattern pattern	Sets the destination pattern.
progress_ind alert strip	Allows the media gateway to send a 180 ringing instead of 183 progress SDP. Used to fix RBT generation issues.
port *voice-port*	Specifies the voice port, which should be used to route the call
forward-digits all	Specifies that all digits will be forwarded to the endpoint connected to FXS port.

13.1.5 CUCM Configuration

Below are the steps necessary in order to configure a connection to a VG in a non-standard architecture.

SIP Trunk configuration (*Device -> Trunk*):

Parameter	Value
Trunk Type	SIP Trunk
Device Protocol	SIP
Trunk Service Type	Default
Device Name	TRK-<Site>-<VG Name>
Description	SIP trunk to specific VG
Device Pool	DPO-SIPTRK-<Site>
Location	LOC-<Site>
Call Classification	OnNet
Media Resource Group List	< None >

SRTP Allowed	Not Checked
Run On All Active Unified CM Nodes	Not Checked
Call Routing Information – Inbound Calls	
Significant digits	All
Calling Search Space	CSS-VCGVLG- Enhanced-<CTY><Site>
Redirecting Diversion Header Delivery - Inbound	Checked
Call Routing Information – Outbound Calls	
Calling Party selection	Originator
Redirecting Diversion Header Delivery – Outbound	Checked
Use Device Pool Called Party Transformation CSS	Checked
Use Device Pool Calling Party Transformation CSS	Checked
SIP Information	
Destination Address	<IP address of VG>
Destination Address is an SRV	Not Checked
Destination Port	5060
Rerouting Calling Search Space	CSS-VCGVLG- Enhanced-<CTY><Site>
Out-of-Dialog Refer Calling Search Space	CSS-VCGVLG- Enhanced-<CTY><Site>
SIP Trunk Secure Profile	SIPT-GW
SIP Profile	SIPP-GW
DTMF Signaling Method	RFC 2833

Route Group configuration (*Call Routing -> Route/Hunt -> Route Group*):

Route Group Name	ROG-<Site>-<VG Name>
Distribution Algorithm	TopDown
Selected Devices	TRK-<Site>-<VG Name>

Route List configuration (*Call Routing -> Route/Hunt -> Route List*):

Name	ROL-<Site>-<VG Name>
Description	RL for specific OnNet range to VG SIP controlled device
CUCM Group	CMG01
Enable this Route List	Checked
Run On All Active Unified CM Nodes	Checked
Selected Groups	ROG-<Site>-<VG Name>

Route Pattern configuration (*Call Routing -> Route/Hunt -> Route Pattern*):

Route Pattern	Private Directory Number toward Fax
Route Partition	PAR-Shared
Description	Route Pattern to Fax
Route Class	Default
Gateway / Route List	ROL-<Site>-<VG Name>

Route option	Route this pattern
Call Classification	OnNet
Urgent Priority	Not Checked
Use Calling Party's EPNM	Checked

Translation Pattern configuration (*Call Routing -> Translation Pattern*):

Translation Pattern	Private range toward Fax range i.e. \+4822538.XXXX
Partition	PAR-ForcedOnNet
Description	OnNet calls to VG Fax
Calling Search Space	CSS-AutoAnswer
Route option	Route this pattern
Urgent Priority	Not Checked
Called Party Transformation	
Discard option	Predot
Prefix	InterSite Prefix + SLC (Site Location Code)

13.1.6 CUBE Configuration

In order to enable CUBE IP2IP gateway functionality, following command has to be entered:

```
voice service voip
      mode border-element license capacity [session count]
      allow-connections sip to sip
      sip
          header-passing
          error-passthru
          no update-callerid
        early-offer forced
          midcall-signaling passthru
          sip-profiles 1
             ip address trusted list
                    ipv4 A.B.C.D   ! primary SBC IP address
                    ipv4 E.F.G.H   ! backup SBC IP address
```

Explanation

Command	Description
mode border-element license capacity [session count]	[session count] – indicate the session count based on the license purchased for CUBE
allow-connections sip to sip	Allow IP2IP connections between two SIP call legs
header-passing error-passthru	Error messages are passed through CUBE (SIP error transparency)
no update-callerid	Transparency regarding Caller ID

early-offer forced	Enables SIP Delayed-Offer to Early-Offer globally
midcall-signaling passthru	Passes SIP messages from one IP leg to another IP leg
sip-profiles 1	Apply sip profile at global level

Please note that there is a difference between 12.4T and 15.4(3)M2 trains regarding two commands “header-passing” and “error-passthru”, which should be taken into account while making an update between the two IOS versions. With 12.4T they should be invoked together as “header-passing error-passthru” while in 15.4(3)M2 they should be invoked as 2 separate commands: “header-passing” and “error-passthru”

13.1.6.1 Media Passing through CUBE (media flow-through vs. media flow-around)

Default CUBE configuration enables CUBE to work in flow-through mode. In order to enable flow-around mode, please perform the following actions:

```
voice service voip
   media flow-around
```

13.1.6.2 Codecs

BT/BTIP requires currently monocodec configuration. That means, that only a single codec should be offered by CUBE. This is configured using codec class which is then applied to specific dial-peer.

For customers using **G.711 alaw** codec:

```
voice class codec 1
  codec preference 1 g711alaw
```

For customers using **G.711 ulaw** codec:

```
voice class codec 1
  codec preference 1 g711ulaw
```

13.1.6.3 SIP user agent

SIP signaling parameters are configured in the sip user agent section.

```
sip-ua
   retry invite 1
   retry response 2
   retry bye 2
   retry cancel 2
   reason-header override
   connection-reuse
   g729-annexb override
   timers options 1000
```

Explanation

Command	Description
retry …	Specifies number of retries for different SIP message types
reason-header override	Enable cause code passing from one SIP leg to another
connection-reuse	Always use the same port for both source and destination (UDP 5060)
g729-annexb override	Required for interoperability with BT/BTIP infrastructure, when G.729 codec is used

13.2 Integrating Sagem XMedius Fax Server Enterprise 9.0 with CUCM

In this section, we will present the steps necessary to integrate Sagem XMedius fax server with Cisco Unified Communications Manager (CUCM).

The XMediusFAX Enterprise edition is field proven to manage large fax volumes and deliver high levels of security, advanced integration, and monitoring & reporting capabilities. It is targeted for small and large enterprises and contains a number of key features.

13.2.1 Highlights for Sagem XMediusFax Server Enterprise 9.0:

- XMediusFAX is Sagemcom's innovative and patented IP fax server solution supporting the robust and standardized T.38 Fax over IP (FoIP) protocol.
- Direct SIP trunking with BTIP
- Simplified application integration through standardized technologies (i.e. XML, Python, Web Services API)
- Business critical system monitoring through application SNMP traps and PerfMon counters
- SQL database scalable to millions of inbound / outbound faxes with easy archiving
- Enhanced LDAP directory integration (i.e., Active Directory, Lotus Domino) with LDAPS support
- Intelligent fax boards and T.38 support
- Virtual machine support using VMware, Microsoft Hypervisor and Citrix
- Supported Document Formats: Adobe PDF, HTML, JPG, GIF, RTF, Microsoft Word, PowerPoint, Excel, Any Windows application that support "Print-To".
- Monitor all faxes sent, received, or in process, as well as server status
- Live graphical fax port usage monitor and integrated network packet capturing utility
- Email notification of service status events to administrator via SMTP
- Administrative audit logging and application services status changes logged in Windows Event Log
- System queue monitoring and alerts through SNMP and Performance Monitor (PerfMon)

- Integrated system reporting with a comprehensive set of 20+ built-in reports
- SSL authentication and encryption between all server modules and clients
- HTTPS for secured Web Client communications
- Built-in Windows Authentication support
- Support for LDAP over SSL (LDAPS)
- Enforce usage of billing codes
- Restricted destination fax number tables
- Per user/profile security settings (Allow to fax, require password, modify sender information, enforce cover page)

13.2.2 Supported fax features with BTIP Service

Please refer to the roadmap, the restriction portal and the INA synopsis portal for more information. List of supported features by XMediusFax Server Enterprise:

- Fax calls using G.711 a-law, G.711 u-law OR G.729 codec can only be proposed in case of specific offers (monocodec configuration – only one codec can be used in WAN for each customer)
- Send fax using XMediusFax SendFax desktop application
- Send fax using XMediusFax Web Panel application
- Incomming fax traffic
  - From standard G3/SG3 Fax machines
- Outgoing fax traffic
  - To standard G3/SG3 Fax machines.
- Sagem XmediusFax server can send G3 or SG3. This is global setting declared in license file and cannot be change without obtaining new license file.

13.3 Sagem XMediusFax Server components configuration

Creating a Profile

Immediately after installation, the **Basic** and **No Faxing Rights** profiles are available, to which you can associate users.
The **Basic profile** allows the user to fax at a normal fax priority, with three retries if a connection cannot be immediately established
The **No Faxing Rights profile** does not allow the transmission of faxes.

You might also create new profiles and assign them to meet the specific fax needs of each user. It is also possible to create different profiles for each department, thereby tailoring fax settings to departmental requirements rather than user requirements.

In the MMC Snap-in, select the **Profiles** node of your site, and click on the **Add** button.The **Profile Properties** dialog appears.

Parameter Name	Parameter Value
❶ Enter the name of the profile In the **Profile Name** field.	❶ for example: Sagem XMF Warsaw
❷ Select the **Phone Books** tab. If you want to assign phone books to the profile: - In the **Phone Books** section, click **Add**. The **Phone Book Properties** dialog appears. - Select a phone book in the **Phone Book** dropdown list. **Note:** A phone book must have been previously created. To create and populate a phone book refer to the **Administration Guide – Web** documentation.	❷ for example: 3580000
❸ Select the **Billing Codes** tab to **Associating a Profile and a Billing Group** - Once billing groups have been created, administrators can associate a billing group with a profile. The billing group can contain any number of billing codes and sub-billing codes which users can apply when faxing.	❸ Default values are used
❹ Click the **Fax Options** tab to set the fax priority and how it affects the order in which the faxes are sent. This is however compounded by the number of retry attempts to send a fax.	❹ Default values are used

❺ Select the **Security** tab to apply security settings. ❻ Select the **Notification** tab to set Notifications. By default, incoming fax notifications are sent to the destinations in the **Incoming Routing Table**, or to the default destination specified in its properties. Outbound fax notifications are sent to the sender's e-mail address.	❺ Default values are used ❻ Default values are used

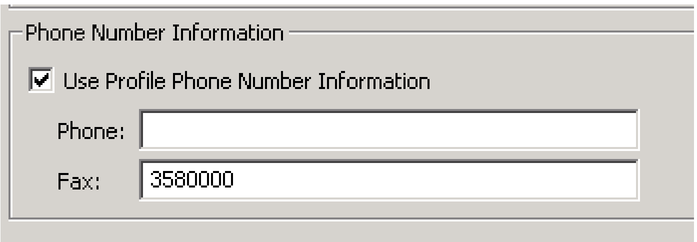
Sagem XMediusFax number presentation on SIP trunk

Configuration of number presentation on SIP trunk from XMF to CUCM. **Number presentation** – this number will be included in SIP INVITE message send by Sagem server, for example:

SIP INVITE SDP() → *SIP From: sip:**3580000**@XMF_IP:5060*

Sites > Site_name > Configuration > Profiles > Profile properties > Profile tab > **Phone Number Information** section

Parameter Name	Parameter Value
❶ Phone Number Information section > Select **Profile Phone Number Information** checkbox	❶ checkbox must be enabled
❷ In **Fax** field provide phone number "extension" compliant with XMF dialplan	❷ for example: 3580000
❸ **Phone** field can be empty, not required to provide phone number	❸ empty value



Phone Number Information

☑ Use Profile Phone Number Information

Phone:

Fax: 3580000

Picture 2: Phone Number Information configuration in Profile

Creating an Internal User Account

In the administration interface, select the **Internal User** node of your site and click on the **Add** button. The **User Properties** dialog appears.

Parameter Name	Parameter Value
❶ Enter the **SMTP address** of the user; this is a mandatory entry.	❶ 3580001@orange-multimedia.fr
❷ Use **Profile Name** to associate the user to a specific profile. **Note:** A profile is mandatory. If no profile exists, you can choose Basic or No Faxing Rights. If you want to create a new profile, refer to **Step 1**. **Tips:** If the SMTP user has a corresponding Windows Domain account, use **AD account** to indicate that account in the format **domain\username**.	❷ Profile Name: **Basic**
❸ Navigate to **Personal Information** tab in User Properties windows. Provide **Phone Number Information** details (Phone number and Fax number) for new user. Must be compliant with XMF dial plan.	❸ Personal Information example: Phone: **3580001** Fax: **3580001**

T.38 Driver Properties Configuration (Options, T.38, SIP)

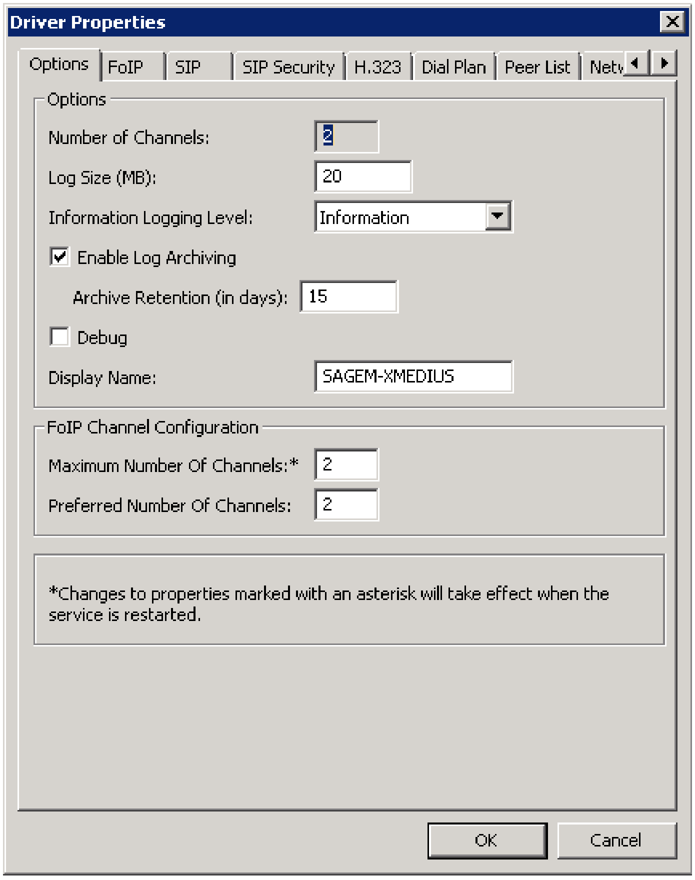
In the administration interface, you just need to access the properties of the Driver node of your host to configure general SIP properties and to configure SIP specific properties for listed gateways and associate number patterns to specific gateway.

Warning: Parameters locations on Driver Properties tabs can be different. It depends on T.38 driver release installed on the server.

System Configuration > **Hosts** > **XMF_Host_name** > **Driver** container > Right Mouse Button click on **Driver** container and select **Properties**. In the **Driver properties** dialog, select the **Options** tab.

Parameter Name	Parameter Value
❶ On **Options** tab enable **Enable Log Archiving** property**.** Enables automatic log archiving for future support use.	❶ Checkbox **Enable Log Archiving** must be enabled. Set **Archive Retention** (in days) to value: **15.**
❷ On **Options** tab **Debug** checkbox should be disabled.	❷ Disabled
❸ On **Options** tab the T.38 Channel Configuration Section configuration.	❸ When you acquire a new license, you need to update here the number of channels allowed according to this new license

❹ On **FoIP** tab configure ECM (error correction mode).	❹ ECM may be enabled (Enabled ECM checkbox) or disabled. It depends on customer requirements. **If Enabled:** • **Received Document Encoding** set to **Group 3 (1d)** • **Terminal Resolution Capacity** set to **High (200x200)**
❺ In the **Driver properties** dialog, select the **SIP** tab. Provide port number under which SIP messages are received for UDP, TCP and TLS.	❺ The general SIP properties are the following • Local SIP UDP Port - **5060** • Local SIP TCP Port - **5060** • Local SIP TLS Port – **5061** • Print SIP Messages – **Disabled** • Wait For DTMF Code Input - **Disabled**


Driver Properties

Options

Number of Channels: 2

Log Size (MB): 20

Information Logging Level: Information

☑ Enable Log Archiving

Archive Retention (in days): 15

□ Debug

Display Name: SAGEM-XMEDIUS

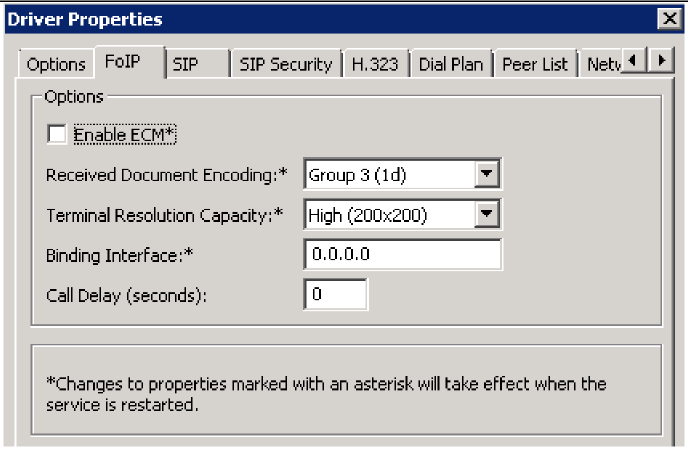
FoIP Channel Configuration

Maximum Number Of Channels:* 2

Preferred Number Of Channels: 2

*Changes to properties marked with an asterisk will take effect when the service is restarted.

Picture 5: Example of Driver Configuration (Options tab)



Driver Properties

Options

□ Enable ECM*

Received Document Encoding:* Group 3 (1d)

Terminal Resolution Capacity:* High (200x200)

Binding Interface:* 0.0.0.0

Call Delay (seconds): 0

*Changes to properties marked with an asterisk will take effect when the service is restarted.

Picture 6: Example of Driver Configuration (FoIP tab) with Disabled ECM

Note: If XmediusFAX is installed in high availability mode driver settings must be configured on all nodes visible in hosts list.

T.38 Driver Properties Configuration (Managing a Dial Plan and Peer List)

By default, XMediusFAX assumes that all faxes are to be sent through a single gateway. The list SIP gateways (in our case it will be CUCM), called the Peer List, therefore displays the single gateway established when XMediusFAX

was installed. The corresponding dial plan indicates that all numbers will use the only gateway available.

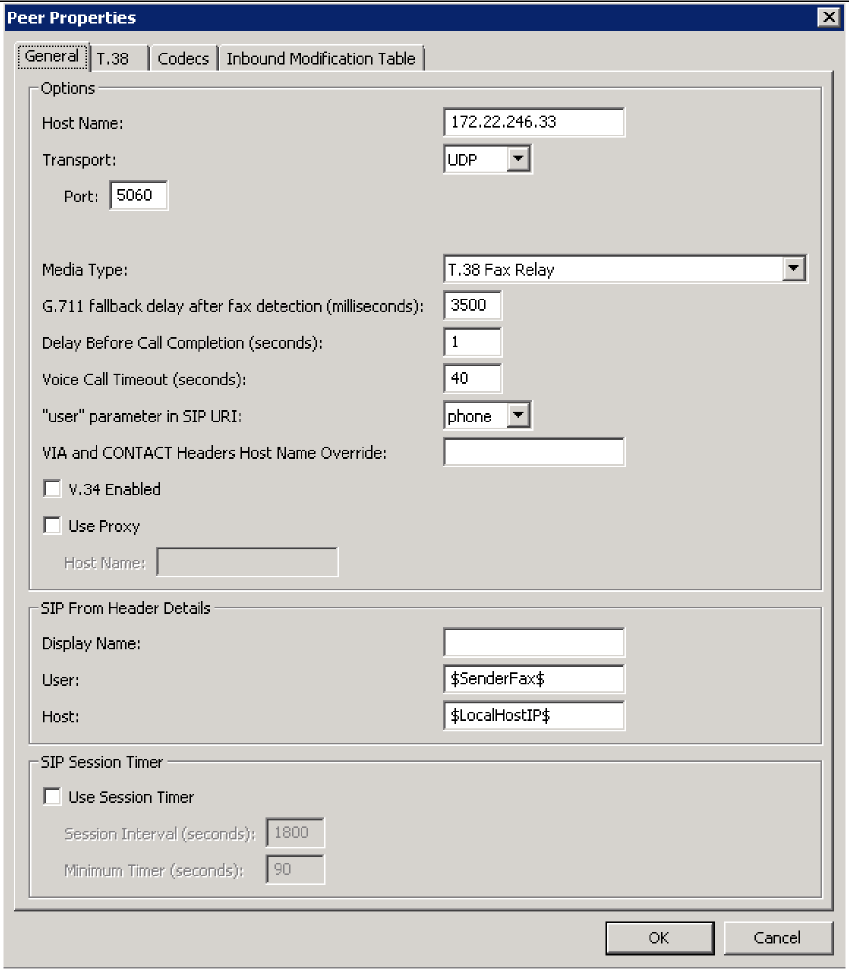
By using a Peer List, you can manage separately the SIP or H.323 properties to use for each known gateway (or proxy) that communicate with the fax server.

System Configuration > **Hosts** > **XMF_Host_name** > **Driver** container > Right Mouse Button click on **Driver** container and select **Properties**.

In the **Driver properties** dialog, select the **Peer List** tab.

Parameter Name	Parameter Value
❶ Click **Add SIP Peer** button. Adds a new SIP Peer and allows to configure its properties	❶ Checkbox **Enable Log Archiving** must be enabled. Set **Archive Retention** (in days) to value: **15**. ❷ IP address of CUCM, for example: **6.5.6.1**.
❷ On **General** tab of Peer Properties window provide **Host Name** - The host name of the gateway (or proxy) to be added as a Peer.	❸ Transport: **UDP**

❸ On **General** tab of Peer Properties window provide the transport type (UDP, TCP or TLS) to be used by this Peer. ❹ On **General** tab of Peer Properties window provide the port number of this Peer. ❺ On **General** tab of **Delay Before Call Completion, Voice Call Timeout and SIP From Header Details.** ❻ On **T.38** tab of Peer Properties window configure **Outbound Initial Media Offer** and **CNG** options. ❼ On **T.38** tab of Peer Properties window configure **Delay before Re-INVITE.** ❽ On **T.38** tab of Peer Properties window configure properties of the **T38 redundancy** section. ❾ On **Codecs** tab click **Add** button to choose codec from **Available Codecs** list.	❹ 5060 ❺ Delay Before Call Completion – **1 second** Voice Call Timeout – **40 seconds** Display name – **empty** User - **$SenderFax$** Host - **$LocalHostIP$** ❻ Outbound Initial Media Offer -**Audio** CNG - **Send CNG using RPT** ❼ Delay before Re-INVITE - **2 seconds** ❽ LS redundancy (possible range 0-2) – **2** HS redundancy (possible range 0-2) – **1** ❾It depends on codec requirements, three supported possibilities by Orange Infrastructure: - **G.711 A-Law 8 kHz** - **G.711 u-law 8 kHz** - or G.729 8kHz



Options

Host Name: 172.22.246.33

Transport: UDP

Port: 5060

Media Type: T.38 Fax Relay

G.711 fallback delay after fax detection (milliseconds): 3500

Delay Before Call Completion (seconds): 1

Voice Call Timeout (seconds): 40

"user" parameter in SIP URI: phone

VIA and CONTACT Headers Host Name Override:

□ V.34 Enabled

□ Use Proxy

Host Name:

SIP From Header Details

Display Name:

User: $SenderFax$

Host: $LocalHostIP$

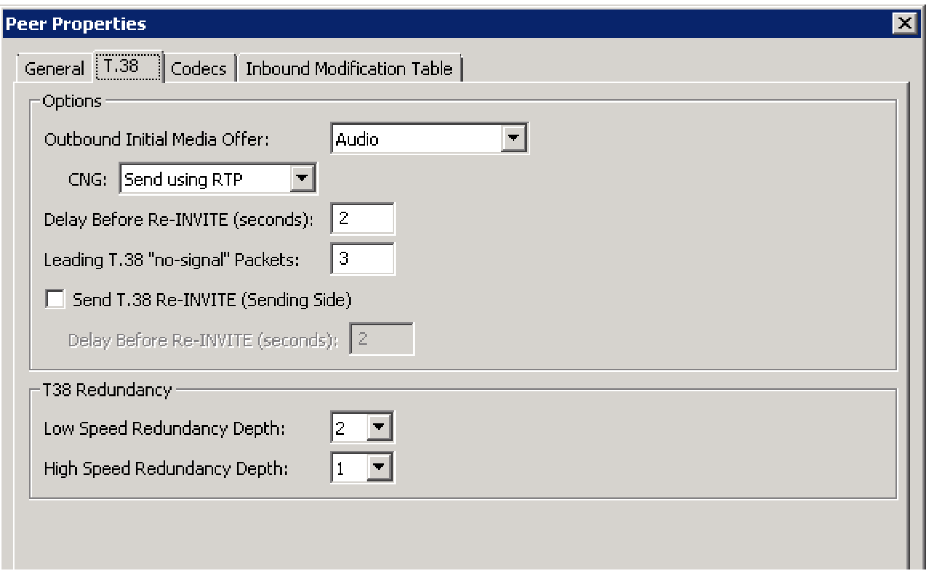
SIP Session Timer

□ Use Session Timer

Session Interval (seconds): 1800

Minimum Timer (seconds): 90

Picture 7: Example of Driver Configuration – new Peer SIP From Headers configuration



Options

Outbound Initial Media Offer: Audio

CNG: Send using RTP

Delay Before Re-INVITE (seconds): 2

Leading T.38 "no-signal" Packets: 3

□ Send T.38 Re-INVITE (Sending Side)

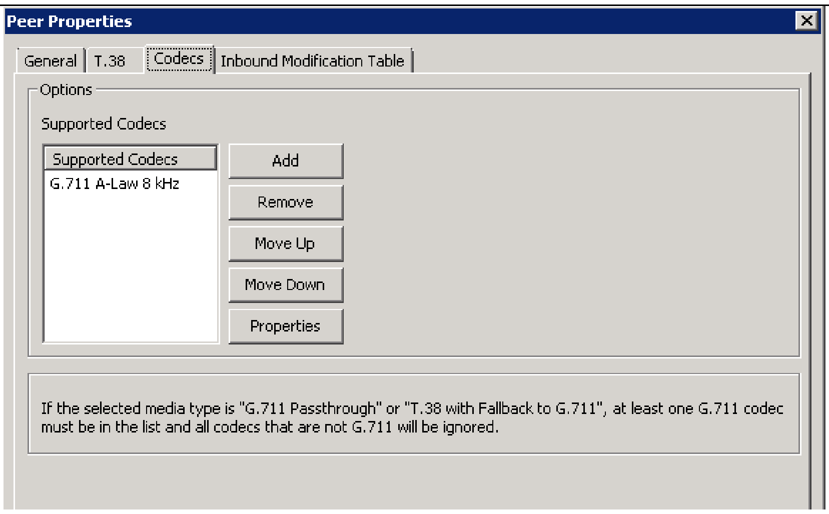
Delay Before Re-INVITE (seconds): 2

T38 Redundancy

Low Speed Redundancy Depth: 2

High Speed Redundancy Depth: 1

Picture 8: Example of Driver Configuration - new Peer



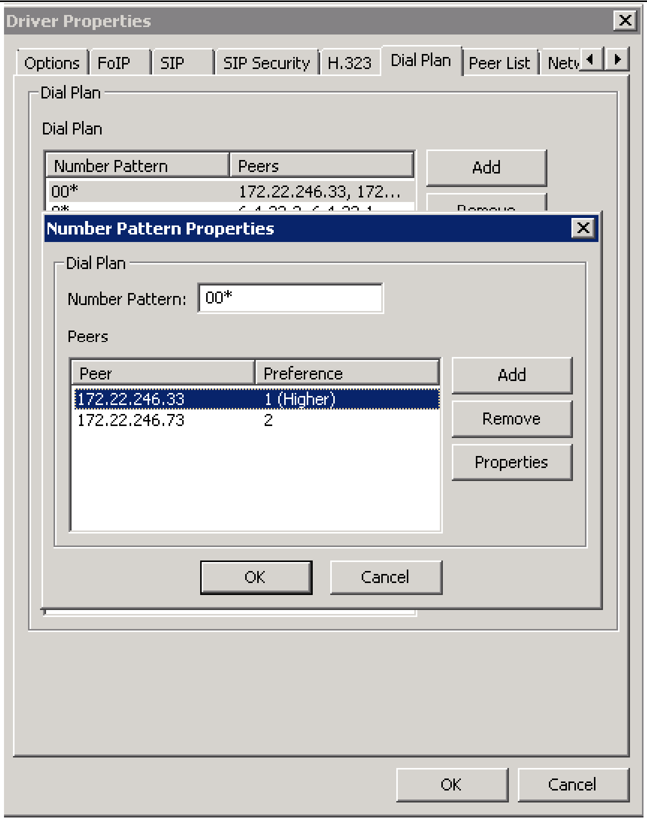
Supported Codecs: G.711 A-Law 8 kHz

If the selected media type is "G.711 Passthrough" or "T.38 with Fallback to G.711", at least one G.711 codec must be in the list and all codecs that are not G.711 will be ignored.

Picture 9: Example of Driver Configuration – new Peer Codec

In the **Driver properties** dialog, select the **Dial Plan** tab.

Parameter Name	Parameter Value
❶ Click **Add** button. Provide **number pattern** you wish to associate with the list of Peers below.	❶ *** (asterisk)** **Note:** You must specify the entire fax number anticipated. Wildcards can be entered: - The asterisk (*) specifies any number of digits - The question mark (?) specifies a single digit.
❷ Select a Peer to Add to the List Associated with a Number Pattern. Click Add button to select configured Peer (Orange SBC).	❷ Peer: **6.5.6.1** **Preference: 1 (Higher)**
❸ On **General** tab of Peer Properties window provide the transport type (UDP, TCP or TLS) to be used by this Peer.	❸ Transport: **UDP**



Dial Plan

Number Pattern	Peers
00*	172.22.246.33, 172...

Number Pattern: 00*

Peers

Peer	Preference
172.22.246.33	1 (Higher)
172.22.246.73	2

Picture 10: Example of Driver Configuration – Dial Plan configuration

Note: If XmediusFAX is installed in high availability mode driver settings must be configured on all nodes visible in hosts list.

Incoming routing table (System Configuration)

XMediusFax > System Configuration > Hosts > Incoming Routing Table

In the MMC Snap-in, select the **Incoming Routing Table** node and then click **Add**. The **Routing Table Entry Properties** dialog appears

Parameter Name	Parameter Value
❶ Enter a valid DNIS/DID number in the Lower Bound field.	❶ 3580000
❷ Enter a valid DNIS/DID number in the Upper Bound field.	❷ 3580099 **Note:** The **Lower Bound** and **Upper Bound** values must have the same amount of digits and the **Upper Bound** value must be higher than the **Lower Bound** value. ❸ Site : **Sagem**

❸ Select the site to which you want to associate these values, from the list in the **Site** field. ❹ Enter the site Call Station ID in the **CSID** field.	❹ CSID : **sagem**

13.3.1 CUCM Configuration

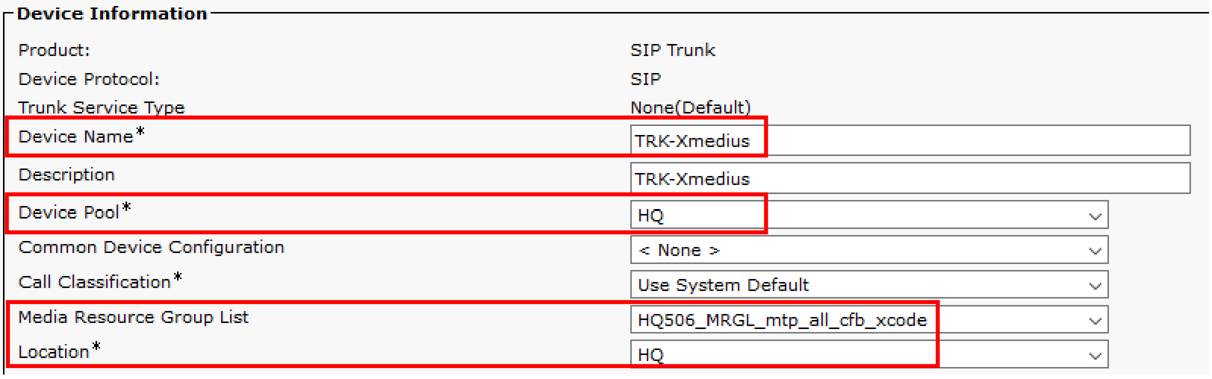
This section describes the steps necessary to take on CUCM in order to integrate it with Sagem Xmedius Fax server.

13.3.1.1 SIP Trunk Configuration

Go to Device -> Trunk and click Add New. On next page, select following options:

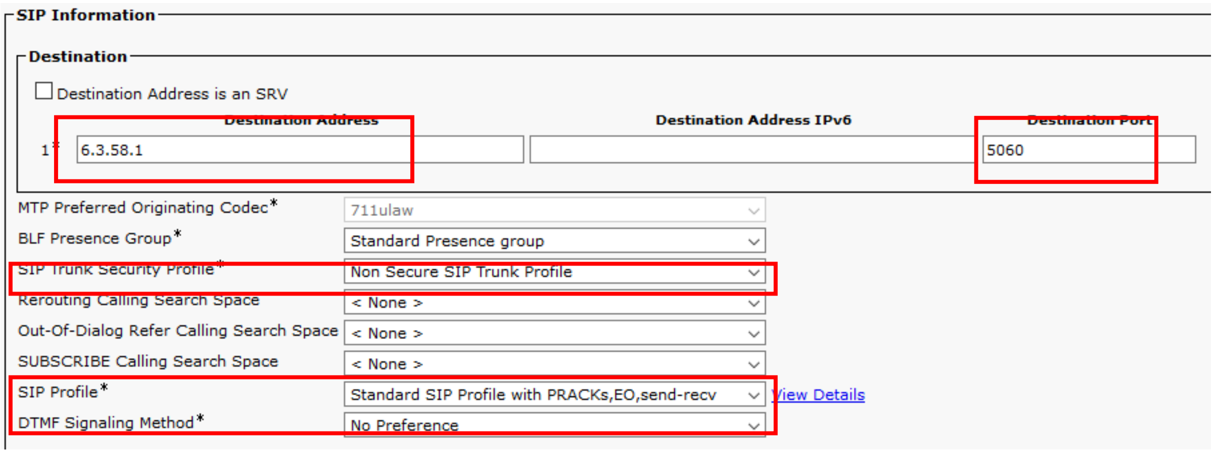
- **Trunk Type:** SIP Trunk
- **Device Protocol:** SIP
- **Trunk Service Type:** None (Default)

Click Next. In next window, configure following options:



Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	TRK-Xmedius
Description	TRK-Xmedius
Device Pool*	HQ
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	HQ506_MRGL_mtp_all_cfb_xcode
Location*	HQ



SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	6.3.58.1		5060

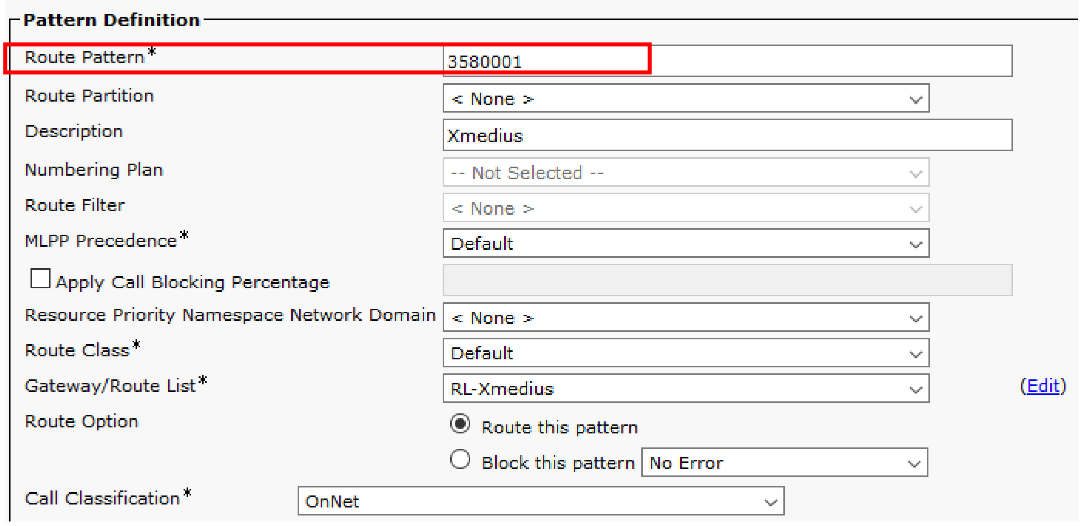
MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile with PRACKs,EO,send-recv View Details
DTMF Signaling Method*	No Preference

Setting	Value	Description
Device Name	TRK-Xmedius	Name of SIP Trunk
Device Pool	HQ	Device Pool, to which this SIP Trunk belongs
Media Resource Group List	MRGL_MTP_XCODE	Select MRGL which has MTPs, transcoders and other standard media resources.
Destination Address	IP Address of Sagem Xmedius	Specify the IP address of Sagem Xmedius Fax server
Destination Port	5060	Specify the port, which will be used for communication, 5060 is default one.
SIP Trunk Security Profile	Non-Secure SIP Trunk Profile	Standard, built-in SIP Trunk Security Profile.
SIP Profile	Standard SIP Profile with PRACKs, EO, send-recv	Standard SIP Profile.
DTMF Signalling Method	No Preference	Chooses any compliant method of DTMF signals transport.

Select Save - this finishes configuration of SIP Trunk.

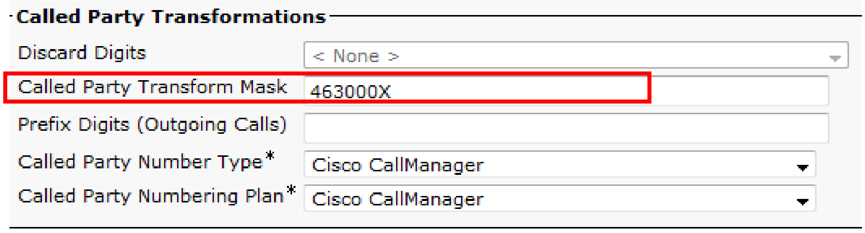
13.3.1.2 Route Pattern Configuration

In order to have calls routed to Sagem Xmedius, we need to configure the dial-plan element which will allow this. Go to Call Routing -> Route/Hunt > Route Pattern. Click Add New button and configure following options:



Pattern Definition

Route Pattern*	3580001
Route Partition	< None >
Description	Xmedius
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	RL-Xmedius (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error
Call Classification*	OnNet



Called Party Transformations

Discard Digits	< None >
Called Party Transform Mask	463000X
Prefix Digits (Outgoing Calls)	
Called Party Number Type*	Cisco CallManager
Called Party Numbering Plan*	Cisco CallManager

Setting	Value	Description
Route Pattern	Depends on deployment Here: 3580001	Dialed number that will be directed to Sagem Xmedius fax server.
Called Party Transform Mask	Depends on deployment Here: 463000X	Called number to which originally dialed number will be transformed to. Can be left blank if no change required.

Confirmation tests

13.4 Validation overview

The complete FAX gateway/endpoint validation consists of

1. Functional tests – mix of tests using G3 and Super G3 machines in both directions. Engineering confirms overall page transmission quality (visual comparison) and technical aspects like T38 profile, transmission speed, T30 negotiation and fallback to G3.

2. Statistical tests – stress tests of device. FaxLab application connected to ChannelTrap simulators repeats fax calls many times to confirm device stability in longer period of time.

13.5 Validation

13.5.1 Functional

It is a list of incoming and outgoing FAX calls going through **Business Talk** infrastructure. Following tests should be done using **non empty page** (full text or simple image).

Test Distribution		
Direction	**Gateway**	**PSTN Fax**
Incoming	G3	G3
Outgoing	G3	G3
Incoming	SG3	G3
Outgoing	SG3	G3
Incoming	G3	SG3
Outgoing	G3	SG3
Incoming	SG3	SG3
Outgoing	SG3	SG3

13.5.2 Statistical

Statistical tests have been done to confirm live implementation stability. Statistical session as described in following table:

Type of calls		Number of pages
Fax type	**Direction**	**10p**
G3	Incoming	100x
	Outgoing	100x
SG3	Incoming	100x
	Outgoing	100x