

Integration of Oracle SBC with Analog Devices and Microsoft Teams Direct Routing

**Technical Application Note** 





#### Disclaimer

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

## Contents

1	REVI	ISION HISTORY	5
2	INTE	ENDED AUDIENCE	5
3	RELA	ATED DOCUMENTATION	5
	3.1	ORACLE SBC	5
	3.2	MICROSOFT TEAMS	5
4	VALI	IDATED ORACLE VERSIONS	6
5	ABO	UT TEAMS DIRECT ROUTING	6
6	INFR	ASTRUCTURE REQUIREMENTS	7
7	CON	FIGURATION	7
	7.1	PREREQUISITES	
	7.2	ABOUT SBC DOMAIN NAME	9
8	CON	FIGURE DIRECT ROUTING	
	8.1.1	Access Teams Admin Center	
	8.1.2	Configure Online PSTN Gateway	
	8.1.3	Configure Online PSTN Usage	
	8.1.5	Configure Online Voice Route	
	8.1.6	Configure Voice Routing Policy	
	8.1.7	Assign Voice Routing Policy to Users	
9	ORA	CLE SBC CONFIGURATION	
	9.1	GLOBAL CONFIGURATION ELEMENTS	14
	9.1.1	System Config	
	9.1.2	Media Manager	
	9.1.3	Sip Config	
	9.2	NETWORK CONFIGURATION	
	9.2.1	Physical Interfaces	
	9.2.2	Network Interfaces	
	9.3	SECURITY CONFIGURATION	
	9.3.1	Certificate Records	
	9.3.2	SBC End Entity Certificate	
	9.3.3	TLS Profile	
	9.3.4	Media Security Configuration	
	9.3.5	Saes-profile	
	9.3.0	TRANSCODING CONFICURATION	
	9.4	I RANSCODING CONFIGURATION	
	9.4.1	Codec Policies	
	9.4.2	PTCP Policy	
	9.4.5	Ice Profile	
	95	MEDIA CONFIGURATION	
	951	Realm Config	
	952	Steering Pools	22
	9.6	SIP CONFIGURATION	
	9.6.1	SIP Profile	

///X

	24
9.6.2 Sip Feature	
9.6.3 Sip Interface	35
9.6.4 Session Agents	
9.6.5 Session Agent Group	
9.7 ROUTING CONFIGURATION	
9.7.1 Local Policy Configuration	
10 VERIFY CONNECTIVITY	42
10.1 OCSBC Options Ping	
10.2 MICROSOFT SIP TESTER CLIENT	42
11 SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS	43
11.1 Terminology	
11.2 REOUIREMENTS FOR INVITE MESSAGES	
11.2.1 Contact Header	
11.3 REQUIREMENTS FOR OPTIONS MESSAGES	44
11.3.1 Contact Header	44
12 MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS	44
13 SIP ACCESS CONTROLS (MANDATORY FOR MSFT TEAMS)	46
14 APPENDIX A	
14.1 SBC BEHIND NAT SPL CONFIGURATION	
15 CAVEATS	49
15.1 No Audio-On-Hold	
16 RUNNING CONFIGURATION	50

11%

#### 1 Revision History

Version	Date Revised	Description of Changes
1.0	04/17/2019	Initial publication
1.1	01/07/2022	Removed reference to sip-all FQDN
1.2	09/13/2022	Added Cert-record for DigiCert Global G2 Cert Added Access-Control
1.3	02/12/2024	Updated requirements for SBC's end entity certificate
1.4	07/20/2024	Removed reference to ping- response parameter and added notes for using tIs-global config in ACLI

#### 2 Intended Audience

This document describes how to connect Analog Devices and the Oracle SBC to Microsoft Teams Direct Routing. This paper is intended for IT or telephony professionals.

Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.

#### 3 Related Documentation

#### 3.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- https://docs.oracle.com/cd/F12246\_01/doc/sbc\_scz830\_security.pdf

#### 3.2 Microsoft Teams

- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure</u>
- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users</u>
- <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc</u>

#### 4 Validated Oracle Versions

Microsoft has successfully conducted testing with the Oracle Communications SBC versions:

SCZ830

Please visit <u>https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers</u> for further information.

These software releases with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- VME

#### 5 About Teams Direct Routing

Microsoft Teams Direct Routing allows a customer provided SBC to connect to Microsoft Phone System. The customer provided SBC can be connected to almost any telephony trunk or interconnect 3rd party PSTN equipment. The scenario allows:

- Use virtually any PSTN trunk with Microsoft Phone System;
- Configure interoperability between customer-owned telephony equipment, such as 3rd party PBXs, analog devices, and Microsoft Phone System

#### 6 Infrastructure Requirements

#### The table below shows the list of infrastructure prerequisites for deploying Direct Routing.

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	
SIP Trunks connected to the SBC	
Office 365 tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	See Microsoff's Plan Direct Pouting document
Public DNS entry for the SBC	See microsoft's <u>Flan Direct Nouting</u> document
Public trusted certificate for the SBC	
Firewall ports for Direct Routing signaling	
Firewall IP addresses and ports for Direct Routing media	
Media Transport Profile	
Firewall ports for client media	

#### 7 Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Teams Direct Routing Interface.

Below shows the connection topology example for MSFT Teams Carrier Model. There are multiple connections shown:

- Teams Direct Routing Interface on the WAN
- Service provider Sip trunk terminating on the SBC
- Third Party ATA (Analog) device
- Third Party IP PBX (optional to use as registrar for ATA)

Note: Oracle did not implement a third party IP-PBX during the certification testing of analog devices with Microsoft Teams. The configuration outlined below demonstrates use of third party ATA (analog device) over secure transport direct to the Oracle SBC without registration or authentication.





Oracle SBC with Microsoft Teams Media Bypass and ATA Remote Worker

These instructions cover configuration steps for the Oracle SBC and Microsoft Teams Direct Routing Interface. The configuration of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.

#### 7.1 Prerequisites

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name for each registered subdomain representing individual tenants using the multitenant Direct Routing Trunk. Each FQDN must resolve to the Public IP address
- Public certificate, issued by one of the supported CAs (refer to <u>Related Documentation</u> for details about supported Certification Authorities).



The SBC domain name must be from one of the names registered in "Domains" of the tenant. You cannot use the **\*.onmicrosoft.com** tenant for the domain name. For example, on the picture below, the administrator registered the following DNS names for the tenant:.

DNS Name	Can Be Used For SBC	Example of FQDN names
		Valid FQDN:
		<ul> <li>customers.telechat.o- test06161977.com</li> </ul>
		Sbc51. telechat.o-test06161977.com
	YES	<ul> <li>Ussbc15. telechat.o- test06161977.com</li> </ul>
telechat.o-test06161977.com		Europe. telechat.o- test06161977.com
		Invalid FQDN:
		<ul> <li>Sbc1.europe.telechat.o- test06161977.com (this would require registering domain name "Europe.adatum.biz")</li> </ul>
solutionslab.onmicrosoft.com	NO	Using *.onmicrosoft.com domains is not supported for SBC names

Below is an example of registered DNS names in the customer tenant.

#### telechat.o-test06161977.com

Note: The above FQDN's are examples only and not to be used outside of this document. Please use FQDN's that are applicable to your environment.

	Microsoft 365 admin cent	ter		
		< Home	e > Domains	
ŵ	Home		View All domains	Q
8	Users	$\sim$	Domain name	Status
ጽ	Groups	^	telechat.o-test06161977.com (Default)	Setup complete
	Groups		customers.telechat.o-test06161977.com	Setup complete
	Billing	$\checkmark$	solutionslab.onmicrosoft.com	Setup complete

For the purposes of this example, the following IP address and FQDN is used:

FQDN Names	Public IP Address
telechat.o-test06161977.com	141.146.36.68

#### 8 Configure Direct Routing

The steps outlined below is the minimum required configuration to pair your SBC with Microsoft Teams Direct Routing Interface. This is to be used as an example only, and we highly recommend you work with your Microsoft Account representative to implement the correct configuration for your specific environment.

#### 8.1.1 Access Teams Admin Center

The first step is to access the <u>Teams Admin Center</u> with administrator admin credentials:

Sign in				
Sign in				
testing@solutionslab.o	nmicrosoft.com			
Can't access your account				
Sign in with a security key	0			
	Back	Next		
	Can't access your account? Sign in with a security key	Can't access your account? Sign in with a security key ⑦ Back	Can't access your account? Sign in with a security key ⑦ Back Next	Can't access your account? Sign in with a security key ⑦ Back Next

## 8.1.2 Configure Online PSTN Gateway

	Microsoft Teams adn	nin center			
			Direct Routing \ Add SBC		
ඛ	Dashboard				
දුටු	Teams	$\sim$	telechat.o-test06161977.com		
۵	Devices	~	You must use the SBC's FQDN that has the host name registere {exampleDomain2} is good name for the SBC, but {exampleDom	d in DNS. For example, if your organization owns {exampleDomain1} then nain3} isn't. {link}	
٢	Locations	$\sim$	SBC settings		
දී	Users		When you are adding this SBC, you can turn on or off	the SBC and change settings that are specific to the SBC.	
÷	Meetings	~	Enabled	On	
Ę	Messaging policies		SIP signaling port	5061	
₿	Teams apps	$\sim$	Sand CID antipat		
ବ	Voice	~	Send SIP options ()	<b>O</b> n	
	Phone numbers		Forward call history	On On	
	Emergency policies		Forward P-Asserted-Identity (PAI) header 🛈	On On	
	Dial plans		Concurrent call capacity	500	
	Direct Routing		Failover response codes	408, 503, 504	
	Voice routing policies		Failover time (seconds) ①	10	
	Call queues		Preferred country or region for media traffic	Auto	~
	Auto attendants		SBC supports PIDF/LO for emergency calls	Off Off	
	Call park policies		Ring phone while trying to find the user	On	

Configuration Path: Voice/Direct Routing/SBC

• Click Save at the bottom of the page

## 8.1.3 Configure Online PSTN Usage

Configuration Path: Voice/Direct Routing/Manage PSTN usage Records (top right of screen)

Click Add, Type US and Canada, next, click Apply

	Microsoft Teams admin cer		
			PSTN usage records
		Direct Routing	Voice routes are linked to voice policies using PSTN usage records. You can manage the list of existing PSTN usage records or add new ones.
ĉĈ	Networks & locations Users	Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more	4 items
ŧ			+ Add
Ę	Messaging policies	Direct routing summary	US and Canada



	Microsoft Teams admin center			
			oice routes \ Oracle_US	
ඛ	Dashboard			
දීරී	Teams	$\sim$	Oracle_US	
\$	Devices	$\sim$	Description	
٢	Locations	$\sim$		
දී	Users		Priority	1
Ē	Meetings	~	Dialed number pattern	^(\+1[0-9]{10})\$
Ę	Messaging policies			
ß	Teams apps	~	SBCs enrolled	
ବ	Voice	^	Select which SBC's you want calls to route to. All SBC's that you	add will be tried in a random order.
	Phone numbers		Add/remove SBCs 1 item	
	Emergency policies		(	
	Dial plans		✓ SBCs	
	Direct Routing		sbc2.customers.telechat.o-test06161977.com	
	Voice routing policies			
	Call queues		PSTN usage records	
	Auto attendants		The voice routing policy is linked to a voice route using the PST in which the voice routing should be processed and assign the	N usage records below. You can add existing PSTN usage records, change the order nolicy to users
	Call park policies			
	Calling policies		✓ Add/remove PSTN usage records 1° Move up ↓	Move down 1 item
	Caller ID policies		✓ PSTN usage record	
le sterer (	Policy packages	arc	✓ US and Canada	

Configuration Path: Voice/Direct Routing/Voice Routes

## 8.1.6 Configure Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies

	Microsoft Teams admin o	enter
	≡	Voice routing policies \ US Only
ഹ	Dashboard	
දීලී ි	Teams ~	US Only
\$	Devices ~	Add a friendly description so you know why it was created
٢	Locations $\sim$	
දී	Users	PSTN usage records
Ë	Meetings ~	PSTN usages are linked to both voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they are listed until a match is found.
E	Messaging policies	
BŶ	Teams apps V	Add/remove PSTN usage records ↑ Move up ↓ Move down 1 item
ଚ	Voice ^	✓ PSTN usage record
	Phone numbers	✓ US and Canada

## 8.1.7 Assign Voice Routing Policy to Users

Configuration Path: Users/Select the "User"/Policies

Next to Voice Routing Policy, Click Edit and Assign. In this example, we have selected Teamsuser1:

	Microsoft Teams admi	in center		
		=		
~	D		Assigned policies 🖉 Edit	Policy package 🖉 Edit
ហ	Dashboard			
සී	Teams	$\sim$	RestrictedAnonymousAccess	Package assigned None
ا	Devices	$\sim$	Mercaning policy	
0	Lesstions		Global (Org-wide default)	
U	Locations	Ť.	live events policy	
ti	Users		Global (Org-wide default)	
Ē	Meetings	$\sim$	App permission policy	
Ē	Morraging policies		Global (Org-wide default)	
2	messaging policies		App setup policy	
B	Teams apps	$\sim$	Global (Org-wide default)	
6	Voice	$\sim$	Call park policy	
ه	Policy packages		Call park	
Ľ	Toncy packages		Calling policy	
<b>4</b> 11	Analytics & reports	$\sim$	Global (Org-wide default)	
ු	Org-wide settings	$\sim$	Caller ID policy	
~=	01		Anonymous	
	Planning	~	Teams policy	
S	Legacy portal 🖸		Global (Org-wide default)	
	Call quality dashboard		Emergency calling policy	
			Global (Org-wide default)	
			Emergency call routing policy	
			Global (Org-wide default)	
			Dial plan	
			Global (Org-wide default)	
			Voice routing policy	
			Oracle_US	

For More Information about configuring Microsoft Teams to Connect to your SBC, Setting up users, or configuration voice routing, please refer to the <u>Related Documentation</u> Section of this guide.

#### 9 Oracle SBC Configuration

There are two methods for configuing the OCSBC, ACLI or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the <u>ACLI configuration guide</u>.

To access the OCSBC GUI, enter the management IP address into a web brower. When the login screen appears, enter the username and password to access the OCSBC.

Once you have accessed the OCSBC, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.

# Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for connection to MSFT Teams Direct routing or Analog device to function properly.

Please note, the below configuration example assumes Media Bypass is enabled on the MSFT Teams Tenant. This configuration example is based on the latest OCSBC software release, SCZ830M1P8A, which contains new parameters designed to simply the SBC's configuration for Microsoft Teams. If running a release prior to SCZ830m1p8A, please refer to <u>Configuring the Oracle SBC with Microsoft Teams Direct Routing Media Bypass</u> <u>– Enterprise Model</u> for instruction on how to configure.

	nfiguration Monitor and Trace Widgets	s System										
🗐 Save 🌣 Wizards - 🏟 Commands -												
Objects	Configuration objects											
media-manager	Name	Description										
security	access-control	Configure a static or dynamic access control list										
session-router	account-config	Configure Quality of Service accounting										
system	account-group	Configure accounting group										
	allowed-elements-profile	Configure allowed elements profiles										
	audit-logging	Configure audit-logging parameters										

#### 9.1 Global Configuration Elements

Before you can configuration more granular parameters on the SBC, there are three global configuration elements that must be enabled to proceed.

- System-Config
- Media-manager-Config
- Sip-Config

#### 9.1.1 System Config

To configure system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)

ORACLE		
Home	Configuration Monitor and Trace	Widgets System
🖶 <u>S</u> ave 💠 Wizards - 🖨 Comman	ds <del>-</del>	
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify System config	
security	Hostname:	telechat.o-test06161977
<ul> <li>session-router</li> <li>system</li> <li>capture-receiver</li> </ul>	Description:	Teams Carrier Model OCSBC
fraud-protection	Location:	Bedford, MA
nost-route network-interface	Mib system contact:	
network-parameters	Mib system name:	
ntp-config	Mib system location:	
phy-interface redundancv-config	Acp TLS profile:	×
snmp-address-entry	SNMP enabled:	•
snmp-community	Enable SNMP auth traps:	
snmp-group-entry	Enable SNMP syslog notify:	
snmp-user-entry snmp-view-entry	Enable SNMP monitor traps:	
spl-config	Enable env monitor traps:	
system-access-list	Enable mblk_tracking:	
system-config	Enable 12 miss report	

• Click the OK at the bottom of the screen

#### 9.1.2 Media Manager

To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

ACLI Path: config t→media-manager→media-manager-config

The following options are recommeded for global media manager when interfacing with MSFT Teams Direct Routing

- Options: Click Add, in pop up box, enter the string: audio-allow-asymmetric-pt
- Click Apply/Add Another, then enter: xcode-gratuitous-rtcp-report-generation (requires a reboot to take effect)
- Max-Untrusted-Signalling=1
- Min-Untrusted-Signalling=1
- Hit OK in the box

ORACLE			
Home	Configuration Monitor and Trace Wi	dgets System	
🗐 Save 🌣 Wizards - 🔅 Comman	ids •		
<ul> <li>Objects</li> <li>media-manager codec-policy dns-alg-constraints dns-config</li> </ul>	Modify Media manager State: Flow time limit:	✓ 86400	(Range: 04294967295)
ice-profile media-manager media-policy	Subsq guard timer:	300	(Range: 04294967295) (Range: 04294967295)
msrp-config playback-config	TCP initial guard timer: TCP subsq guard timer:	86400 300 300	(Range: 04294967295) (Range: 04294967295) (Range: 04294967295)
realm-group rtcp-policy	Hnt rtcp: Algd log level:		▼
static-flow steering-pool tcp-media-profile	Mbcd log level: Options:	NOTICE Add   Edit   Delete	*
<ul> <li>security</li> <li>session-router</li> <li>system</li> </ul>		audio-allow-asymmetric-pt xcode-gratuitous-rtcp-report-generatio	n

#### 9.1.3 Sip Config

To enable sip related objects on the OCSBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

ACLI Path: config t→session-router→sip-config

The following are recommended parameters under the global sip-config:

- Options: Click Add, in pop up box, enter the string: inmanip-before-validate
- Click Apply/Add another, then enter: max-udp-length=0
- Press OK in box

Home	Configuration Monitor and Trace	Widgets System
📄 <u>S</u> ave 🔅 Wizards - 🔅 Comr	mands <del>-</del>	
Save Wizards - Comm enum-config filter-config h323 home-subscriber-server http-alg iwf-config ldap-config local-policy local-response-map local-routing-config media-profile net-management-control qos-constraints response-map service-health session-agent session-agent session-constraints session-constraints session-group session-recording-group session-recording-server session-timer-profile	mands - Modify SIP config State: Dialog transparency: Home Realm ID: Egress Realm ID: Registrar domain: Registrar domain: Registrar host: Registrar port: Init timer: Max timer: Trans expire: Initial inv trans expire: Invite expire: Session max life limit: Enforcement profile: Red max trans:	Image: Constraint of the second se
session-translation sip-advanced-logging	Options:	Add Edit Delete
sip-config		inmanip-before-validate max-udp-length=0
sip-teature		

Note: If using the SBC in an access environment to register ATA with IP-PBX, please check the <u>Oracle SBC</u> <u>Configuration guide</u> regarding proper setting for home realm, registrar-host, and registrar-port.

• Click OK at the bottom

## 9.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure three physical interfaces, and three network interfaces. One to communicate with MSFT Teams Direct Routing, one to connect to PSTN Network, and a third to communicate with the Analog Device

#### 9.2.1 Physical Interfaces

GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

• Click Add, use the following table as a configuration example:



Note: Physical interface names, slot and port may vary depending on environment

Home Configuration Monitor and Trace Widgets System													
🖶 Save 🌣 Wizards - 🌣 Commands -													
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Phy interface Search Criteria: All	Phy interface Search Criteria: All											
security	Add Edit Copy Delete Delete All Upload Download												
session-router	Name	Operation type	Port	Slot	Virtual mac	Admin state							
system	s0p0	Media	0	0		enabled							
capture-receiver	s1p0	Media	0	1		enabled							
haud-protection	s1p1	Media	1	1		enabled							

• Click OK at the bottom of each after entering config information

#### 9.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

• Click Add, use the following table as a configuration example:

Configuration Parameter	Teams	PSTN	ATA
Name	s0p0	s1p0	S1p0
Hostname	(Optional)		
IP Address	141.146.36.68	192.168.1.10	155.212.214.177
Netmask	255.255.255.192	255.255.255.0	255.255.255.0
Gateway	141.146.36.65	192.168.1.1	155.212.214.1
DNS Primary IP	8.8.8.8		
DNS Domain	Carrier Default Domain		

	nfiguration Monitor and Trace Wid	gets System										
目 <u>S</u> ave 尊 Wizards・ 森 Commands・												
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Network interface Search Criteria: All	Vetwork Interface Search Criteria: All										
security	Add Edit Copy Delete Delete All Upload Download											
session-router	Name	Sub port id	Description	Hostname	IP address							
system	s0p0	0			141.146.36.68							
capture-receiver	s1p0	0			192.168.1.10							
haud-protection	s1p1	0			155.212.214.177							

• Click OK at the bottom of each after entering config information

#### 9.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Teams Direct Routing and ATA interfaces

Microsoft Teams Direct Routing only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one fo the trusted Cerificate Authorities. A list of currently supported Certificate Authrities can be found at:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

#### 9.3.1 Certificate Records

"Certificate-records" are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

For the purposes of this application note, we'll create four certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certificate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certificate signed by this authority)

#### 9.3.2 SBC End Entity Certificate

The SBC's end entity certificate is based on the domain structure outlined in the <u>Configuration</u> section of this document. This certificate record must include the following:

- Common name: SBC Domain Name (telechat.o-test06161977.com)
- Extended Key Usage List: serverAuth clientAuth

To Configure the certificate record:

• Click Add, and configure the SBC certificate as shown below:

ORACLE	Configuration	Monitor and Trace	Widgets St	vstem	
	comguration	monitor and made	magets 5	Jacin	
🗐 <u>S</u> ave 🔅 Wizards - 🎎 Co	ommands -				
Objects	Modify C	ertificate record			
media-manager					
security	Name:		TeamsEn	nterpriseCert	
admin-security	Country	y:	US		
auth-params	State:		California		
authentication	Locality		California		
authentication-profile	Locality	y.	Redwood	d City	
cert-status-profile	Organiz	zation:	Oracle C	orporation	
certificate-record	Unit:				
insec	Commo	on name:	telechat.c	o-test06161977.com	
media-security	Key siz	e:	2048		
password-policy	Alterna	te name:	2040		
public-key	Tracting				
security-config	Trusted	1:			
ssh-config	Key usa	age list:	Add	Edit Dele	te
tls-global			digitalSig	nature	
tls-profile			keyEncip	herment	
session-router					
system					
capture-receiver					
hest route					
http.client	Extende	ed key usage list:	٨dd	Edit Dolo	to
http-crient			Auu	Luit Dele	10
network-interface			ServerAut	th b	
network-interface			ClientAut	n	

- Click OK at the bottom
- Next, using this same procedure, configure certificate records for Root CA and Intermediate Certificates

## 9.3.2.1 Root CA and Intermediate Certificates

#### 9.3.2.1.1 Go Daddy Root

The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

#### 9.3.2.1.2 DigiCert Global Root G2

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by DigiCert Global Root G2.To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2



#### 9.3.2.1.3 Baltimore Root

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

You can download this certificate here: <u>https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem</u>

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	Baltimore Root	GoDaddy Root	DigiCert Global Root G2
Common Name	Baltimore CyberTrust Root	Go Daddy Class2 Root CA	DigiCert Global Root G2
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256

ORACLE Enterprise Session Border Controller														
NN3950-101 10.1	NN3950-101 10.138.194.101 SCZ9.0.0 Patch 3 (Build 290) Dashboard Configuration Monitor and Trace													
Configuration	View Configuration	Q							Discard	😧 Verify	🖹 Save			
media-manager	Þ	Certific	ate Re	ecord										
security	•													
authentication-p	orofile													
certificate-record	d		1. 1	PKCS12					Search		Q			
certificate record	u	Action	Select	Name	Country	State	Locality	Organization	Unit	Comn	non Name			
tls-global		÷		BaltimoreRoot	US	MA	Burlington	Engineering		Baltin	nore CyberT			
tls-profile		:		DigiCertGlobalRootG2	US	МА	Burlington	DigiCert	www.digicert.com	DigiCe	ert Global R			
system	•	:		GoDaddyRoot	US	МА	Burlington	Engineering		GoDa	ddy Class2 F			
		:		SBCCertificateforTea	US	California	Redwood City	Oracle Corporation		telech	at.o-test06'			

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.

ORACL	ORACLE Enterprise Session Border Controller 🔹 admin 🔻														
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 3 (Build 290) Dashboard Configuration Monitor and Trace Widgets														Sy am	
Configuration View Configuration Q												😟 Verity	🖹 Save		
media-manager	•		Certific	ate Re	ecord										
security	v														
authentication-pr	ofile			- •									Count		0
certificate-record			L: Щ т. 🕹 🔟 РКСЯ		PKCS12		Confine					Search		Q	
			Action	Select	Name		Co	Confirm		ocality		Organization	Unit	Comm	ion Name
tis-global			:		Baltimore	Root	US	Do you want to activ	vate the configuration?	urlington		Engineering		Baltim	ore CyberT
tls-profile								Confir	Cancel						
session-router	►		:		DigiCertO	blobalRootG2	US	Comm	Cancer	urlington		DigiCert	www.digicert.com	DigiCe	rt Global R
system	+		:		GoDaddy	Root	US		МА	Burlington		Engineering		GoDad	ldy Class2 F
			:		SBCCerti	ficateforTea	US		California	Redwood City		Oracle Corporation		telech	at.o-test06′

#### 9.3.2.2 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. This is not required for any of the Root CA or intermidiate certificates that have been created.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

ORACL	E En	nterprise Se	ession Bo	rder Co	ntroller							Û 🔺	admin 🔻
NN3950-101 10.13	8.194.101	I SCZ9.0.0	Patch 3 (B	Build 290	)				Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Co	onfiguration	Q								Discard	😟 Verify	🖹 Save
media-manager		•	Certific	ate Re	ecord								
security		•											
authentication-pr	ofile		D: t	<u>n</u> 1	₹	PKCS12		<b>.</b>			Search		Q
certificate-record			Action	Select	Name		Country	State	Locality	Organization	Unit	Comm	on Name
tls-global			:		Baltimore	Root	US	МА	Burlington	Engineering		Baltim	ore CyberT
tls-profile session-router		•	:		DigiCertG	ilobalRootG2	US	МА	Burlington	DigiCert	www.digicert.com	DigiCe	rt Global Re
system		Þ	:		GoDaddy	Root	US	МА	Burlington	Engineering		GoDad	ldy Class2 F
			:		SBCCertif	icateforTea	US	California	Redwood City	Oracle Corporation		telecha	at.o-test06′



Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

#### 9.3.2.3 Import Certificates to SBC

Once certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.

ORACL		Session Bo	order Co	ntroller						Û 🔺	admin 🔻
NN3950-101 10.12	i8.194.101 SCZ9.0	.0 Patch 3 (E	Build 290				Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q							Discard	😧 Verify	🖹 Save
media-manager security	•	Certific	ate Re	ecord							
authentication-p	ofile	D; t	<u>ћ</u> 土	▶ E PKCS12					Search		Q
certificate-record		Action	Select	Name	Country	State	Locality	Organization	Unit	Comn	non Name
tls-global		:		BaltimoreRoot	US	МА	Burlington	Engineering		Baltin	nore CyberT
session-router	Þ	:		DigiCertGlobalRootG2	US	МА	Burlington	DigiCert	www.digicert.com	DigiCe	ert Global Re
system	•	:		GoDaddyRoot	US	MA	Burlington	Engineering		GoDa	ddy Class2 F
		:		SBCCertificateforTea	US	California	Redwood City	Oracle Corporation		telech	at.o-test06'

Format try-all   Import Method  File Paste Paste	Format try-ell   Import Method File  Paste	Format try-all  File Faste Paste Pas	ormat     try-all       mport Method     File       Paste     Paste       aste    BEGIN CERTIFICATE Synoback State       MIIHM/CCBhogAwlBAgIQC3C/hIB HZQ8xkQTv4A0WW2ANBgkqhkiG 9v0BAqSFADB MQavCQYDVQQGEwJVUzEVMB MGAIUEChMMRGInaUNIcnQgSW SJMSku/JWYDVQQUPJB aWapQ2VjvdEBUTTMgUINBINDA TIINIAjWhUNEINBMTAREWOyMTA SMJAwMDAwMDBa FvdQMJASNIgMzUSINTIAMIGkM OswCOYDVOOGEwJVUzETMBEG	aste try-all   File  File  File  Faste  saste  File  File  Sourcestant CERTIFICATE MIIHMICCENtgAwiBAgiOC3C/INB MCGWCVDVOQCGEWJVUzEVMB MCGAUEChMMRGinaLNiknQgSW SMSKuvVDVQODEPADBP MQwCVDVOQCGWJVUzEVMBE SMVDAVDVDVODEPBE SMVDAVDVDVDVDVDVD SMVDAVDVDVDVDVDVD SMVDAVDVDVDVDVDVD SMVDAVDVDVDVDVDVDVD SMVDAVDVDVDVDVD SMVDAVDVDVDVDVDVDVD SMVDAVDVDVDVDVDVDVD SMVDAVDVDVDVDVDVDVD SMVDAVDVDVDVDVDVD SMVDAVDVDVDVDVDVDVD SMVDAVDVDVDVDVDVDVDVDVDVDVDVDVDVDVDVDVDVD	Format try-ell   Import Method  Import Method  File  Paste  Paste Pa	Format try-all  Import Method Import Method File Paste	Format try-all  Import Method Import Method File Paste	Format Import Method Import Method File File Faste Paste MIIHMICCBhagAwiBAgiQC3C/hiB HZQ8xQTV4A0WWANBgkqhriG WG8AQSFADBP MG8AUCQYDVQQCEwJVUEVMB MG8AUCCQYDVQQCEWJVUEVMB MG8AUCQYDVQQCEWJVUEVMB SMSkwJwYDVVQQDEyBE 8W6pQ2VydC8UTHWBUINBIFNQ TIINiAyMDIwHENBMTAEFw0yMTA SMJAwMDAwMDBa Fw0gMJASMigyMzUSNTIaMIGkM OswCOYDVOOGEwJVUzETMBEG	Format Import Method Import Method File File Faste Paste MIHMICCBhagAwiBAgiQC3C/hiB HZQ3xkQTvAA0WWAANBgkqhkiG WQavCQYDVQQCEwJVUzEVMB MGAuCQYDVQQCEwJVUzEVMB MGAUCQYDVQQDEyBE WGQVQVdCBUTHAUNicnQsSW SJMSkwJwrDVVQDEyBE WGQVJdCBUTHAUNicnQsWATA SMAAWADAwMDBa FivQyMJASMigyMzUSNTIaMIGkM OswCOYDVOOGEwJVUzETMBEG	Import Certificate			
Import Method File Paste Paste	Import Method File Paste Paste Past	Import Method File Paste	nport Method File Paste aste BEGIN CERTIFICATE MIHM/CCBhagAwlBAgIQC3C/hB HZQBwkQTvAA0WVzANBgrchhiG WQBAQcFADBP MQswCQVVQQGEwJVUzEVMB MGAIUEChMMRGinaUNicnQgSW SJMSkwJWDQWDEyBE aWldpQZVydCBUTFMgUINBIFNQ TINIAyMDMieIBBAThaFw0QMTA SMJAWMDAwMDBa Fv0QMJMDMieIBBAThaMliGkM QswCOYDVOOGEwJVUzETMBEG	nport Method File Paste aste	Import Method File Paste Pas	Import Method File Paste Pas	Import Method File Paste Pas	Import Method File Paste	Import Method File File Faste Faste Faste File File File File File File File Fil	Format	try-all	•	
Paste Paste	Paste Paste Paste  MIHM/CCBhogAwlBAgIQC3C/hIB HZQ8xkQTv4A0WWzANBgkqhkiG 9w0BAQsFADBP MQswCQYDVQQC6cwJVUzEVMB	Paste Page Paste Page Page Page Page Page Page Page Page	Paste aste    BEGIN CERTIFICATE MIIHM/CCBhgAwlBAgIQCSC/HB HZQ8xkQTv4A0WW2ANBgkqhkliG 9w0BAgCAFADBP MQswCQYDVQQEGwJVUzEVMB MGAIUECHMMRGInaUMRcMgSW SIMSkwJw/DVQQDEyBE aWdpQ2VydCBUTFMgUINBIFNIQ TIINAyMDIwIENBMTAFerv0yMTA SMjawMDawMDBa Fw0yMfJAMJgM2WSTNTAMIGkM OswCOYDVQOGEwJVUzETMBEG	Paste  aste    BEGIN CERTIFICATE MIIHM/CCBhq2AwlBAgIQC3C/hB H2Q8k/074AQWIV2ABBqchkiG 9w0BAQFADBP MQswCQVDVQQGGwJVUJzEVMB MGaIUEChMMRGinaLNicnQSW SMSkuvVDVQQDEB aWapQ2VydCBUTFMgLINBIFNIQ TINBkyMVDVQDVPDBB aWapQ2VydCBUTFMgLINBIFNIQ SMJAwMDAwMDBa Fw0yMJASMigyMzUSNTIaMIGkM OswCQYDVOOGGwJVUJzETMBEG	Paste	Paste	Paste	Paste	Paste	Import Method	⊖ File		
	MIIHM(CCBhqgAwlBAgl(CSC/hl8 HZQ8xkQVv4A0WWzANBgkqhkiG 9w0BAQsFADBP MQswCQYDVQQGEwJVUzEVMB	MIIHMICEBhqaAwiBAgiQESC/hiB HZQBxkQTv4A0WWZANBgkqhkiG 9w0BAQsFADBP MQswCQYDVQQEwJVU2EV/MB MGATUEChMMRGinaUNicnQgSW 5jM5kwJwYDVQQDEyBE aWaqo2VydCBUTFMgUINBIFNIQ TIINIAyMDiwIENBMTAeFw0yMTA	MillHMjCCBhagAwiBAgIQC3C/hi8 HZQ3x4Q7vA0WW2ANBgknhiG 9w0BAQ5FADBP MQ3wCQDVQQGEwJVU2EVMB MGATUECMMMRGinaUNIcnQgSW 5MSKwJWYDVQQDEVBE aWidpQ2VydCBUTFMgUINBIFNIQ TTINiAyMDWMDBA Fw0QMASMigyMzUSNTIAMIGkM GawCOYDVOOGEwJVU2ETMBEG	MillHMjCCBhagAwlBAgIQC3C/hl8 HZQ5kxGVr4AOWWANBQ5knhiG 9vv0BAQ5FADBP MQsvCQDVQQGEwJVU2EVMB MGaTUEChMMRGinaUNEnQg5W 5MSKswJW7DVQQDEVBE aWdqQ2VydCBUTFMgUINBIFNIQ TTINiAyMMbi/ENSMTAFerwQyMTA 5MjAwhDawMDaa FwQyMJASMgyMzUSMTAMIGkM 0swCQYDVOOGEwJVU2ETMBEG	MIIHM/CCBhagAwiBAgiQCSC/HB HZQBwkQTvAA0WV=XABkqhkiG 9v0BAQeFADBP MQswCQVVQQGEwJVUzEVMB MGAIUEChMMRGinaUNicnQSW SjMSkwJwVDQQDEVBE aWapQ2VycCBUTFMgUINBIFNQ TITINAMDiwIENBMTAFEwOyMTA SMjAwMDAwMDBa FvoQMJAMigNaUSSNTIAMIGKM OswCOYDVOOGEwJVUzETMBEG	MIIHM(CGBnggAwiBAgiQCSC/HB HZQBwKQTvAA0WVARABkqhhiG 9v0BAQsFADBP MQswCQVVQQGEwJVUzEVMB MGAIUEChMMRGinaUNIcnQSW 5jMSkwJwVPOVQQDEVBE aWabQ2VycGBUTFMgUINBINQ TIINAyMDMwHBNBATAFEwOyMTA 5MjAwMDAwMDBa Fw0yMjASMjgyMzUSNTIaMIGKM OswCOYDVOOGEwJVUzETMBEG	MIIHM(CGbng2AwlBAgIQCSC/hl8 HZQ38kQTvAQUW2ANBkqhhlG 9v08AQcFADBP MQswCQVVQQGEwJVU2EVMB MGAIUEChMMRGInaUNIcnQSW 5jMSkuvVVVQQQDEV aWlapQ2VyqCBUTFMcUINBINQ TIINiAyMDInvENBMTAeFw0yMTA 5MJAwMDAvMDBa Fw0yMJA5MjgyMzU5NTIaMIGkM OswCOYDVOOGEwJVU2ETMBEG	MIHMICCBhagAwiBAgiQCSC/hB HZQBAkQTAADWVARBkqhhiG 9v0BAQsFADBP MQswCQVVQQGEwJVUzEVMB MGAIUEChMMRGinaUNIcnQSW 5jMSkuvJVVQQDEVBE siMSbuvJVVQQDEVBE siMsbuvJDWQDEVBE siMsbuvMDAvMDBa Fw0yMJASMigyMzJSNTIaMIGkM OswCOYDVOOGEwJVUzETMBEG	MIHMICCBhagAwiBABIQCSC/HB HZQBAKQTvAA0WVARBkqhhiG 9V0BAQcFADBP MQswCQVVQQGEwJVUzEVMB MGAIUEChMMRGinaUNIcnQSW 5JM5kwJWVQQDEVBE aWabQ2VycCBUTFMcUINBINQ TIINAyMDWKPIBMTAErw0yMTA 5MjAwMDawMDBa Fw0yMASMigyMzUSNTIaMIGkM OswCOYDVOOGEwJVUzETMBEG	Paste	Paste     Paste     CERTIFICATE		

111/11/2

• Once pasted in the text box, select Import at the bottom, then save and activate your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

#### 9.3.3 TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

• Click Add, use the example below to configure

ORACL	E Ent	erprise	Session Border Controller						Û 🗕	admin 🔫
NN3950-101 10.1	38.194.101	SCZ9.0	1.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Con	figuratior	Q					Discard	😟 Verify	🖹 Save
media-manager	)		Modify TLS Profile							
security authentication-p certificate-record tts-global tts-profile session-router system	rofile 1	•	Name End Entity Certificate Trusted Ca Certificates Cipher List Verify Depth Mutual Authenticate TLS Version Options	TLSTeams SBCCertificateforTeams BaltimoreRoot X DigiCertGlobalRootG2 X GoDaddyRoot X DEFAULT X 10 enable tlsv12	( Range: 010 )					•
			ОК	Bark						

• Select OK at the bottom

Next, we'll move to securing media between the SBC and Microsoft Teams.

#### 9.3.4 Media Security Configuration

This section outlines how to configure support for media security between the OCSBC and Microsoft Teams Direct Routing.

#### 9.3.5 Sdes-profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured. The only crypto-suite option supported by Microsoft is AES\_CM\_128\_HMAC\_SHA1\_80 and must be included in the crypto list

GUI Path: security/media-security/sdes-profile

ACLI Path: config t→security→media-security→sdes-profile

• Click Add, and use the example below to configure

ORACLE	Configuration Monitor and Trace	Nidaets System	
🗐 Save 🏟 Wizards - 🏟 Com	mands •		
<ul> <li>Objects</li> <li>media-manager</li> <li>security</li> <li>admin-security</li> </ul>	Modify Sdes profile Name: Crypto list:	SDES	
auth-params authentication cert-status-profile certificate-record ike ipsec media-security		AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80	
dtls-srtp-profile media-sec-policy sdes-profile	Srtp auth: Srtp encrypt: SrTCP encrypt:	2 2 2	
sipura-profile password-policy	Mki:		_
security-config ssh-config tls-global tls-profile	Egress offer format: Use ingress session params:	same-as-ingress  Add   Edit   Delete	
<ul> <li>session-router</li> <li>system</li> </ul>			
	Options:	Add   Edit   Delete	
	Key: Salt: Srtn rekey on re invite:		
	Lifetime:	31	(Range: 0, 2048)

Note: The lifetime parameter set to a value of 31 is required if utilizing Media Bypass on Microsoft Teams

• Click OK at the bottom

#### 9.3.6 Media Security Policy

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Microsoft Teams, the other for non secure media facing PSTN.

GUI Path: security/media-security/media-sec-policy

ACLI Path: config t→security→media-security→media-sec-policy

• Click Add, use the examples below to configure

ORACLE <sup>®</sup>	lome Configuration Monitor and Trac	e Widgets System
📄 Save 🔅 Wizards - 🔅 C	Commands -	
<ul> <li>Objects</li> <li>media-manager</li> <li>security</li> <li>admin-security auth-params authentication cert-status-profile certificate-record</li> <li>ike</li> <li>ipsec</li> </ul>	Modify Media sec policy Name: Pass through: Options:	¢desPolicy Add Edit Delete
<ul> <li>media-security dtls-srtp-profile</li> <li>media-sec-policy</li> <li>sdes-profile</li> <li>sipura-profile</li> <li>password-policy</li> <li>public-key</li> <li>security-config</li> <li>ssh-config</li> <li>tls-global</li> <li>tls-profile</li> </ul>	Inbound Profile: Mode: Protocol: Hide egress media update Outbound Profile:	SDES
<ul> <li>session-router</li> <li>system</li> </ul>	Mode: Protocol:	sdes

21111110

11 %

ORACLE		
Но	me Configuration Monitor and Trace	Widgets System
📙 <u>S</u> ave 🖨 Wizards - 🎝 Co	mmands +	
Objects	Modify Media sec policy	
media-manager		
security	Name:	RTP
admin-security	Pass through:	,
auth-params authentication	Options:	Add   Edit   Delete
cert-status-profile		
certificate-record		
🕨 ike		
ipsec		
media-security		
dtls-srtp-profile		
media-sec-policy		
sdes-profile	Inbound	
sipura-profile	Profile:	
password-policy	Mode:	rtp
public-key	Protocol:	none
security-config	Hide egress media undate:	
ssh-config	nue egress media apuate.	
tis-global	Outbound	
tls-profile	Profile:	
session-router	Moder	
system	wode.	rtp
	Protocol:	none

• Click OK at the bottom of each when applicable

#### 9.4 Transcoding Configuration

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions, and can connect two voice streams that use different coding algorithms with one another.

#### 9.4.1 Media Profiles

For different codecs and media types, you can setup customized media profiles that serve to police media values and define media bandwidth policies.

SILK & CN offered by Microsoft teams are using a payload type which is different usual, so to support this, we configure media profiles on the SBC.

GUI Path: session-router/media-profile

ACLI Path: config t→session-router→media-profile

Configure three media profiles to support the following:

- Silk Wideband
- Silk Narrowband
- CN
- Click Add, then use the table below as an example to configure each:

Parameters	Silk-1	Silk-2	CN
Subname	narrowband	wideband	wideband
Payload-Type	103	104	118
Clock-rate	8000	16000	0

ORACLE	me Co	nfiguration Monitor and Trace Wid	gets System				
<u>■</u> Save ⇔ Wizards • ⇔ Co	mmands	3 <b>*</b>					
<ul> <li>Objects</li> <li>media-manager</li> <li>security</li> </ul>	*	Media profile Search Criteria: All Add   Edit   Copy   E	Delete   Delete All   Upload   Down	load			
session-router		Name	Subname	Media type	Payload type	Transport	Clock rate
access-control		CN	wideband	audio	118	RTP/AVP	0
account-config		SILK	narrowband	audio	103	RTP/AVP	8000
allowed-elements-profile		SILK	wideband	audio	104	RTP/AVP	16000

• Click OK at the bottom of each when applicable

#### 9.4.2 Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the OCSBC the ability to add, strip, and reorder codecs for SIP sessions

Note: This is an optional configuration. Only configure codec policies if deemed necessary in your environment

GUI Path: media-manager/codec-policy

ACLI Path: config t→media-mangaer→codec-policy

Some SIP trunks may have issues with codec being offered by Microsoft teams. For this reason, we have created a codec policy "OptimizeCodecs" for the SIP trunk to remove the codecs that are not required or supported.

Create another codec-policy, addCN, to allow the SBC to generate Comfort Noise packets towards Teams

• Click Add, and use the examples below to configure

ORACLE	Configuration Monitor and Trace	Widgets System
<u>≣ S</u> ave ⇔ Wizards - ⇔ Comm	nands +	
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify Codec policy	
codec-policy	Name:	OptimizeCodecs
dns-alg-constraints dns-config ice-profile media-manager media-policy msrp-config playback-config realm-config realm-group rtcp-policy	Allow codecs:	Add     Edit     Delete       *     6722:no     *       PCMA:no     CN:no     *       SIREN:no     RED:no     *       Add     Edit     Delete
static-flow steering-pool tcp-media-profile security session-router system		PCMU
	Order codecs:	Add Edit Delete
	Packetization time:	20

2/11/10

1/1

	onfiguration Monitor and Trace W	lidaats System
Home Co	monitor and frace in	lugeta System
🗐 Save 🌣 Wizards - 🌣 Command	S <del>•</del>	
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify Codec policy	
codec-policy	Name:	addCN
dns-alg-constraints dns-config	Allow codecs:	Add   Edit   Delete
ice-profile media-manager media-policy msrp-config playback-config realm-config		SILK:no G729:no
realm-group	Add codecs on egress:	Add Edit Delete
rtcp-policy static-flow steering-pool tcp-media-profile security session-router system		CN
	Order codecs:	Add Edit Delete
	Packetization time:	20



## 9.4.3 RTCP Policy

The following RTCP policy needs to be configured for the OCSBC to generate RTCP sender reports toward Microsoft Teams. The <u>media manger</u> options config, xcode-gratuitous-rtcp-report-generation, allows the SBC to generate receiver reports

GUI Path: media-manager/rtcp-policy

ACLI Path: config t→media-manger→rtcp-policy

• Click Add, use the example below as a configuration guide

ORACLE					
	Home C	Configuration	Monitor and Trace	Widgets System	
🗐 Save 🕸 Wizards - 🖨	E Comman	ids <del>-</del>			
<ul> <li>Objects</li> <li>media-manager</li> </ul>		Modify RTCP policy			
codec-policy		Name:		ItcpGen	
dns-alg-constraints		RTCP g	enerate:	all-calls	
ice-profile		Hide cn	ame:		

• Click OK at the bottom

#### 9.4.4 Ice Profile

SBC supports ICE-Lite. This configuration is required to support MSTeams media-bypass.

GUI Path: media-manager/ice-profile

ACLI Path: config t→media-manger→ice-profile

• Click Add, use the example below as a guide to configure

ORACLE	Configuration Monitor and Trace	Widgets System	
📄 <u>S</u> ave 🌣 Wizards - 🍄 Comm	ands -		
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify Ice profile		
codec-policy	Name:	ice	
dns-alg-constraints	Stun conn timeout:	0	(Range: 09999)
dns-config	Stun keep alive interval:	0	(Paper) 0 300)
ice-profile		0	(Kalige: 0500)
media-manager	Stun rate limit:	100	(Range: 099999)

Click OK

Note: Ice Profile should not be configured for Non Media Bypass Environment with Microsoft Teams

#### 9.5 Media Configuration

This section will guide you through the configuration of realms and steering pools, both of which are required for the SBC to handle signaling and media flows toward Teams and PSTN.

#### 9.5.1 Realm Config

In this example, we will configure a realm facing Microsoft Teams, A realm for PSTN Sip Trunk, and a third realm to interface with the ATA or analog device

GUI Path; media-manger/realm-config

ACLI Path: config t→media-manger→realm-config

• Click Add, and use the following table as a configuration example for the three realms used in this configuration example

Config Parameter	Teams Realm	ATA	PSTN Realm
Identifier	Teams	ATA_Realm	SIPTrunk
Network Interface	s0p0:0	S1p1:0	s1p0:0
Mm in realm	$\checkmark$	$\checkmark$	$\checkmark$
Teams-FQDN	Telechat.o-		
	test06161977.com		
Teams fqdn in uri	$\checkmark$		
Sdp inactive only	$\checkmark$		
Media Sec policy	sdespolicy	sdespolicy	RTP
RTCP mux	$\checkmark$		
ice profile	ice		
Codec policy	addCN	OptimizeCodecs	OptimizeCodecs
RTCP policy	rtcpGen		
Access Control Trust Level	High	High	High

The "Teams FQDN" Field is required to allow sip messages generated by the SBC to be formatted according to MSFT Teams Requirements. The SBC FQDN must be configured either in this realm parameter, or under the hostname field of the network interface.

Also notice, the realm configuration is where we assign some of the elements configured earlier in this document, ie...

- Network interface
- Media security policys
- Ice profile (Only required with Media Bypass set to enabled in Direct Routing Interface)
- Codec policys
- Rtcp policy

Home Configuration Monitor and Trace Widgets System						
🗐 Save 🔅 Wizards - 🔅 Command	ls -					
Objects     media-manager     codec policy	Realm config Search Criteria: All	Delate Delate All Unite	ad Download			
dns-alg-constraints	Identifier	Delete Delete All Opio	Addr prefix	Network interfaces		Mm
dns-config ice-profile					In realm	In network
media-manager	ATA_Realm SIPTrunk	Realm Facing Analog Device Realm Facing PSTN	0.0.0.0	s1p1:0 s1p0:0	enabled enabled	enabled enabled
media-policy	Teams	Realm Facing MSFT Teams	0.0.0.0	s0p0:0	enabled	enabled

#### 9.5.2 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other will be shared by all parent and child realms facing Teams.

GUI Path: media-manger/steering-pool

ACLI Path: config t→media-manger→steering-pool

• Click Add, and use the below examples to configure

ORACLE Home C	onfiguration Monitor and Trace Wi	dgets System			
🗐 Save 🎄 Wizards - 🎄 Commands -					
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify Steering pool				
codec-policy	IP address:	192.168.1.10			
dns-alg-constraints	Start port:	20000			
ice-profile	End port:	40000			
media-manager	Realm ID:	SIPTrunk 🗸			

ORACLE	me Configuration	Monitor and Trace	Widgets	System	
🗐 Save 💠 Wizards - 🍄 Co	mmands <del>-</del>				
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Modify Ste	ering pool			
codec-policy	IP addres	ss:	141.14	46.36.68	
dns-alg-constraints	Start por	t:	20000		
ice-profile	End port	:	40000		
media-manager	Realm ID	:	Teams	3	~

ORACLE	Home Configu	ration Monitor and Trace	Widgets	System	
🗐 Save 🔅 Wizards - 🔅	Commands -				
<ul> <li>Objects</li> <li>media-manager</li> </ul>	Mo	dify Steering pool			
codec-policy	1	P address:	155.2	12.214.177	
dns-alg-constraints	:	Start port:	2000		
ice-profile	E	End port:	4000		
media-manager	1	Realm ID:	ATA_F	Realm	~

#### 9.6 Sip Configuration

This section outlines the configuration parameters required for processing, modifying and securing sip signaling traffic.

#### 9.6.1 SIP Profile

A sip profile needs to be configured and will be assigned to the Teams sip interface. This parameter is not currently available through the OCSBC GUI, and needs to be configured, and assigned through the OCSBC ACLI.

ACLI Path: config t→session-router→sip-profile

sip-profile	
name	forreplace
redirection	inherit
ingress-conditional-cac-admit	inherit
egress-conditional-cac-admit	inherit
forked-cac-bw	inherit
cnam-lookup-server	
cnam-lookup-dir	egress
cnam-unavailable-ptype	
cnam-unavailable-utype	
replace-dialogs	enabled

#### 9.6.2 Sip Feature

The following sip feature needs to be added to the Configuration of the SBC to enable support for the replaces, allowing for successful consultative transfer:

GUI Path: session-router/sip-feature

ALCI Path: config t→session-router→sip-feature

r						
ORACLE	Home Co	nfiguration	Monitor and Trace	Widgets	System	
🗐 Save 🛱 Wizards - 🍄	Commands	S <b>+</b>				
diameter-manipulation enforcement-profile	*	Add SIP f	eature			
enum-config		Name:		replac	ces	
filter-config		Realm:		Team	s	¥
<ul> <li>n323</li> <li>home-subscriber-server</li> </ul>	r	Suppor	t mode inbound:	Pass		~
http-alg		Require	mode inbound:	Pass		¥
iwf-config		Proxy r	equire mode inbound:	Pass		<b>v</b>
local-policy		Suppor	t mode outbound:	Pass		*
local-response-map		Require	mode outbound:	Pass		×
local-routing-config		Proxy r	equire mode outbound:	Pass		¥

#### 9.6.3 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the OCSBC Receives and sends SIP messages

Configure three sip interfaces, one associated with PSTN Realm, One for Analog Device, and a third for Microsoft Teams direct routing.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to Configure:

Config Parameter	SipTrunk	Teams	ATA
Realm ID	SipTrunk	Teams	ATA_Realm
Sip Proile		forreplace	
Sip Port Config	Sip Trunk	Teams	
Parmeter			
Address	192.168.1.10	141.146.36.68	155.212.214.177
Port	5060	5061	5061
Transport protocol	UDP	TLS	TLS
TLS profile		TLSTeams	TLSAnalog
Allow anonymous	agents-only	agents-only	Agents-only
in-manipulationid		RespondOptions	

Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, ie....

- Sip-Profile
- TLS Profile

ORACLE	Home Co	onfiguration	Monitor and Trace	Widgets	System
🗐 Save 🖨 Wizards - 🛱 Commands -					
enum-config filter-config h323	*	SIP interfa Search Crite Add	ace eria: All   Edit   Copy	Delete	Delete All   Upload   Downl
home-subscriber-serve	er	State		Rea	Im ID
http-alg		enabled		ATA	_Realm
iwf-config		enabled		SIPT	Trunk
Idap-config		enabled		Tear	ms

#### 9.6.4 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the OCSBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent

You will need to configure three Session Agents for the Microsoft Direct Routing Interface

• Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3
Hostname	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.com
Port	5061	5061	5061
Transport method	StaticTLS	StaticTLS	StaticTLS
Realm ID	Teams	Teams	Teams
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Refer Call Transfer	enabled	enabled	enabled

You may need to configure additional session agents as well, for Sip Trunk and ATA. **This will vary widely based on individual environments and how the ATA is being deployed.** For the purposes of this example only...we will configure two additional session agents, one for SIPTrunk, and another for the Third Party Analog Device

Config parameter	Session Agent PSTN	Session Agent ATA
Hostname	68.68.117.67	155.212.214.170
IP-Address	68.68.117.67	155.212.214.170
Port	5060	5061
Transport method	UDP	StaticTLS
Realm ID	SIPTrunk	ATA_Realm
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Refer Call Transfer	enabled	enabled

Home Cor	nfiguration Monitor and Trace	Widgets System					
diameter-manipulation  enforcement-profile enum-config	iameter-manipulation  Accement-profile search Criteria: All num-config Add Edit Copy Delete Delete All Upload Download						
filter-config h323 home-subscriber-server	Hostname 192.168.1.100 sip.pstnhub.microsoft.com	IP address 192.168.1.100	Port 5060 5061	State enabled enabled	App protocol SIP SIP	Realm ID SIPTrunk Teams	
nttp-aig iwf-config Idap-config	sip3.pstnhub.microsoft.com		5061 5061	enabled enabled	SIP SIP	Teams Teams	

• Hit the OK tab at the bottom of each when applicable

## 9.6.5 Session Agent Group

A session agent group allows the SBC to create a load balancing model:

All three Teams session agents configured above will be added to the group.

GUI Path: session-router/session-group

ACLI Path: config t→session-router→session-group

• Click Add, and use the following as an example to configure:

ORACLE		
Home	e Configuration Monitor and Trac	e Widgets System
📕 <u>S</u> ave 🔅 Wizards - 🔅 Com	mands <del>-</del>	
enum-config filter-config	Modify Session group     Group name:	Tanna Gar
h323 home-subscriber-server http-alg iwf-config	Description:	
Idap-config	State:	
local-response-map local-routing-config	App protocol: Strategy:	SIP 🗸
media-profile net-management-control qos-constraints response-map service-health session-agent session-agent-id-rule	Dest:	AddEditDeletesip.pstnhub.microsoft.comsip2.pstnhub.microsoft.comsip3.pstnhub.microsoft.com

• Click OK at the bottom

#### 9.7 Routing Configuration

This section outlines how to configure the OCSBC to route Sip traffic to and from Microsoft Teams Direct Routing Interface, SIPTrunk, and Third Party Analog Device.

The OCSBC has multiple routing options that can be configured based on environment. Since we have only two DID's associated with the analog device, and two DID's assigned to Teams clients in this test environment, we utilized Local Policy Routing performing DID Separation via the TO (Request-URI) Address field in each local policy where applicable.

The DID assignments are as follows:

TeamsUser1: 17814437247

TeamsUser2: 17814437248

ATA Port 1: 17814437383

ATA Port 2: 17814437384

## 9.7.1 Local Policy Configuration

Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy

Please note, the To Address field in local policy matches the Request URI in Sip Messages.

The following local policy routes calls from PSTN and from ATA to Microsoft Teams that match the To Address:

ORACLE"	ome Configuration	Monitor and	I Trace Wid	lgets !	System	
🗐 <u>S</u> ave 🔅 Wizards - 🔅 C	ommands -					
<ul> <li>media-manager</li> <li>security</li> <li>session-router access-control account-config account-group</li> </ul>	▲ Modify Lo To address	cal policy		Add	Edit D	Noto
allowed-elements-profile class-profile diameter-manipulation enforcement-profile enum-config filter-config h323				178144 178144	37247 37248	stelle
home-subscriber-server http-alg iwf-config Idap-config Iocal-policy Iocal-response-map Iocal-routing-config	Source	realm:		Add SIPTrun ATA_Re	Edit   Di ik ialm	elete
media-profile net-management-control qos-constraints response-map	Descrip	tion:		Route T	ō Teams	
service-health	State:			<		
session-agent session-agent-id-rule	Policy p	riority: tributes		none		*
session-constraints	Add	Edit	Conv	Dolot	0	
session-group	Auu	Eult	Dealm	Deleti	Action	Terminet
session-recording-group session-recording-server	sag:Tea	imsGrp	Teams		none	disabled

The Following Routes Calls from PSTN and from MSFT Teams To ATA that match the To Address:

Hor	ne Co	nfiguration	Monitor and	d Trace Wie	dgets	Systen	n		
🗐 <u>S</u> ave 🙀 Wizards - 🙀 Con	mmands	S <b>-</b>							
<ul> <li>media-manager</li> <li>security</li> </ul>	*	Modify Lo	cal policy						
<ul> <li>session-router access-control</li> </ul>		To addr	ess:		Add		Edit	Del	lete
account-config account-group allowed-elements-profile class-profile diameter-manipulation enforcement-profile					178144 178144	37383 37384			
enum-config filter-config h323 home-subscriber-server		Source realm:			Add Teams SIPTrur	 Ik	Edit	Del	ete
http-alg iwf-config Idap-config									
local-response-map local-routing-config media-profile		Descrip	tion:		Route T	o <u>ATA</u>			
net-management-control gos-constraints		State:			<b>~</b>				
response-map		Policy priority:			none				*
service-health		Policy at	tributes						
session-agent		Add	Edit	Сору	Delet	е			
session-agent-id-rule		Next h	op	Realm		Actio	n		Termina
session-constraints		155.212	2.214.170	ATA_Realm	TA_Realm none				disabled

1111111

If the above configured local policies do not match the To Address Field, then the following policy will route all calls from either the Analog Device or From Teams to PSTN:

ORACLE	Home Conf	iguration	Monitor and	d Trace W	idaets '	System		
	Home Com	guruuon	monitor uni		lugets .	o yotom		
📄 <u>S</u> ave 🔅 Wizards - 🌣	Commands -							
<ul> <li>media-manager</li> <li>security</li> </ul>	<b>^</b>	Modify Lo	cal policy					
<ul> <li>session-router access-control</li> </ul>		To addr	To address:			Edit	De	elete
account-config account-group allowed-elements-profi class-profile diameter-manipulation enforcement-profile enum-config filter-config h323	le	Source	realm:		* Add ATA_Re	Edit	De	elete
home-subscriber-serve http-alg iwf-config Idap-config Idap-config	21				Teams			
local-routing-config media-profile		Description:			Route T	O PSTN		
net-management-contr gos-constraints	ol	State:			✓			
response-map		Policy p	riority:		none			~
service-health		Policy at	tributes					
session-agent		Add	Edit	Сору	Delet	е		
session-agent-id-rule		Next b	ac	Realm		Action		Termina
session-constraints		68.68.1	17.67	SIPTrunk		none		disabled

111/11

The SBC configuration is now complete. You can now save and activate the configuration.

ORACLE	Home Configuration	Monitor and Trace	Widgets	System
E Save ☆ Wizards → Cojects	Commands -	-tion objects		
security Do yo config	ou want to activate the guration?		 ( (	Description Configure a Configure Q
acce acco	ctivate Cancel	profile	(	Configure ao Configure al

Move to verify the connection with Microsoft Direct Routing Interface

#### 10 Verify Connectivity

#### 10.1 OCSBC Options Ping

After you've paired the OCSBC with Direct Routing validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing. (Also verify with PSTN and ATA if applicable)

While in the OCSBC GUI, Utilize the "Widgets" to check for OPTIONS to and from the SBC.

• At the top, click "Wigits"

This brings up the Wigits menu on the left hand side of the screen

#### GUI Path: Signaling/SIP/Methods/OPTIONS

ORACLE <sup>®</sup> Enterpris	e Session Border (	Controller						
	•	Method options						
SIP Codecs								
SIP Errors							Refresh Setti	ngs Add to Das
Interface	•	Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Client PerMax
Methods	•	OPTIONS Requests	16	1417	14	18	1644	16
Mathed Ask		Retransmissions	0	0	0	0	8	1
Method Ack		200 OK	16	1417	14	18	1644	16
Method Bye		Transaction Timeouts	0	0	0	0	0	0
Method Cancel		Locally Throttled	0	0	0	0	0	0

 Looking at both the Server Recent and Client Recent, verify the counters are showing OPTIONS Requests and 2000K responses.

#### 10.2 Microsoft SIP Tester Client

SIP Tester client is a sample PowerShell script that you can use to test Direct Routing Session Border Controller (SBC) connections in Microsoft Teams. This script tests basic functionality of a customer-paired Session Initiation Protocol (SIP) trunk with Direct Routing.

The script submits an SIP test to the test runner, waits for the result, and then presents it in a human-readable format. You can use this script to test the following scenarios:

- Outbound and inbound calls
- Simultaneous ring
- Media escalation
- Consultative transfer

Download the script and Documentation here:

Sip Tester Client script and documentation

#### 11 Syntax Requirements for SIP Invite and SIP Options

Microsoft Teams Hybrid Voice Connectivity interface has requirements for the syntax of SIP messages. This section covers high-level requirements to SIP syntax of Invite, Final Responses to Invite and Options messages. The information can be used as a first step during troubleshooting when calls don't go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

#### 11.1 Terminology

- Recommended not required, but to simplify the troubleshooting, it is recommended to configure as in examples as follow
- Must strict requirement, the system does not work without the configuration of these parameters

#### 11.2 Requirements for Invite Messages

Picture 1 Example of INVITE message

INVITE sip:17814437383@telechat.o-test06161977.com;transport=tls SIP/2.0 Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bK3rfq6u10d8f8fonro0k0.1 From: sip:9785551212@ telechat.o-test06161977.com;transport=tls:5061;tag=0A7C0BFE To: <sip: 17814437383@sip.pstnhub.microsoft.com:5061> Call-ID: F3154A1E-F3AE-4257-94EA-7F01356AEB55-268289@192.168.4.180 CSeq: 1 INVITE Content-Length: 245 Content-Type: application/sdp Contact: <sip:9785551212@ telechat.o-test06161977.com;5061;user=phone;transport=tls> Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE User-Agent: Oracle SBC

Picture 2 Example of 200OK Response To Invite:

SIP/2.0 200 Ok FROM:teamsuser2<sip:+17814437248@sip.pstnhub.microsoft.com:5061;user=phone>;tag=42d0638d0b144 TO: <sip:+17814437266@telechat.o-test06161977.com:5061;user=phone>;tag=cc256d730a030200 CSEQ: 1 INVITE CALL-ID: 673d06cb86725ab6a3a4605967b9a174 VIA: SIP/2.0/TLS 52.114.7.24:5061;branch=z9hG4bK772330cd Record-Route: <sip:sip-du-a-as.pstnhub.microsoft.com:5061;transport=tls;lr> Contact: <sip:+17814437266@telechat.o-test06161977.com:5061;user=phone;transport=tls>;sip.ice Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER Server: T7100/1.0 Content-Type: application/sdp Content-Length: 457 Supported: replaces X-MS-SBC: Oracle/NN4600/8.3.0m1p8A

#### 11.2.1 Contact.Header

- Must have the FQDN sub-domain name of a specific Teams tenant for media negotiation.
- Syntax: Contact:: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>
- MSFT Direct Routing will reject calls if not configured correctly

#### 11.3 Requirements for OPTIONS Messages

Picture 2 Example of OPTIONS message

OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0 Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bKumatcr30fod0o13gi060 Call-ID: 4cf0181d4d07a995bcc46b8cd42f9240020000sg52@155.212.214.173 To: sip:ping@sip.pstnhub.microsoft.com From: <sip:ping@sip.pstnhub.microsoft.com>;tag=0b8d8daa0f6b1665b420aa417f5f4b18000sg52 Max-Forwards: 70 CSeq: 3723 OPTIONS Route: <sip:52.114.14.70:5061;Ir> Content-Length: 0 Contact: <sip:ping@telechat.o-test06161977.com:5061;transport=tls> Record-Route: <sip: customers.telechat.o-test06161977.com >

#### 11.3.1 Contact Header

- When sending OPTIONS to the Direct Routing Interface Interface "Contact" header should have SBC FQDN in URI
- hostname along with Port & transport parameter set to TLS.
- Syntax: Contact: sip: <FQDN of the SBC:port;transport=tls>
- If the parameter is not set correctly, Teams Direct Routing Interface will not send SIP Options to the SBC

#### 12 Microsoft Teams Direct Routing Interface characteristics

Table 1 contains the technical characteristics of the Direct Routing Interface. Microsoft, in most cases, uses RFC standards as a guide during the development. However, Microsoft does not guarantee interoperability with SBCs even if they support all the parameters in table 1 due to specifics of implementation of the standards by SBC vendors. Microsoft has a partnership with some SBC vendors and guarantees their device's interoperability with the interface. All validated devices are listed on Microsoft's site. Microsoft only supports the validated devices to connect to Direct Routing Interface. Oracle is one of the vendors who have a partnership with Microsoft.

Category	Parameter	Value	Comments
	SIP Interface FQDN	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
Ports and	SIP Port	5061	
IP	IP Address range for Media	Refer to Microsoft documentation	
	Media port range on Media Processors	Refer to Microsoft documentation	
	Media Port range on the client	Refer to Microsoft documentation	
	SIP transport	TLS	
	Media Transport	SRTP	
<b>T</b>	SRTP Security Context	DTLS, SIPS Note: DTLS is not supported until later time. Please configure SIPS at this moment. Once support of DTLS announced it will be the recommended context AES CM 128 HMAC SHA1 80.	https://tools.ietf.org/html/rfc5763
and	Crypto Suite	non-MKI	
Security	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP mux helps reduce number of required ports
	Supported Certification Authorities	Refer to Microsoft documentation	
	Transport for Media Bypass (of configured)	ICE-lite (RFC5245) – recommended, · Client also has Transport Relays	
		· G711	
		<ul> <li>Silk (Teams clients)</li> </ul>	
	Audio codecs	<ul> <li>Opus (WebRTC clients) - Only if Media Bypass is used;</li> </ul>	
		· G729	
		· G722	
Codecs		<ul> <li>CN</li> <li>Required narrowband and wideband</li> </ul>	
	Other codecs	· RED – Not required	
		DTMF – Required	
		<ul> <li>Events 0-16</li> <li>Silence Suppression – Not required</li> </ul>	

1/1

2/11/1/12

#### 13 SIP Access Controls (Mandatory for MSFT Teams)

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Please note, DDOS values are specific to platform and environment. For more detailed information please refer to the Oracle Communications SBC Security Guide.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

- 1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
- 2. Set the access control trust level on public facing realms to HIGH

Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie...SipTrunk, etc...

GUI Path: session-router/access-control

ACLI Path: config tàsession-routeràaccess-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14 and 52.120.0.0/14.

ORACLE Enterprise Set	ssion Border C	ontroller		
SolutionsLab-vSBC-1 10.1.1.4 SCZ9.0.	0 Patch 2 (Build 1	172)		
Configuration View Configuration	Q			
media-manager	> ^	Modify Access Control		
security	•			
session-router	-	Realm ID	Teams	•
access-control		Description		
account-config				
filter-config		Source Address	52.112.0.0/14	
ldap-config		Destination Address	0.0.0.0	
local-policy		Application Protocol	SIP	•
local-routing-config		Transport Protocol	ALL	
media-profile		Access	permit	•
session-agent		Average Rate Limit	0	
session-group		Trust Level	high	

11111111

• Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

#### 14 Appendix A

#### 14.1 SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling.

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device. Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Teams side SIP interface.

To configure SBC Behind NAT SPL Plug in, Go to session-router->sip-interface->spl-options and input the following value, save and activate.

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

Here HeaderNatPublicSiplfIp is the public interface ip and HeaderNatPrivateSiplfIp is the private ip.

ORACLE				
H	Home Configuration	Monitor and Trace	Widgets	System
🗐 Save 🖨 Wizards - 🖨	Commands -			
diameter-manipulation enforcement-profile enum-config filter-config h323 home-subscriber-server http-alg iwf-config ldap-config local-policy local-roplicy local-routing-config media-profile net-management-contro qos-constraints	<ul> <li>Modify Si TCP na Registr Min reg Registr Route t Secure Uri fqdi Options</li> </ul>	IP interface at interval: ration caching: g expire: ration interval: to registrar: d network: n domain: s:	90 300 3600	d   Edit   Delete
response-map service-health session-agent session-agent-id-rule session-constraints	<b>Spi</b> opt	ions:	Heade	rNatPublicSipIfIp=52.151.236.203,

• This configuration would be applied to each Sip Interface in the OCSBC configuration that was deployed behind a Nat Device

#### 15 Caveats

#### 15.1 No Audio-On-Hold

Microsoft has enabled the ability for the Direct Routing Interface to generate Music when a Teams Client parks or places a call on hold. Since this feature implementation, which currently cannot be disabled, some users have experienced no audio when trying to retrieve calls in which hold or park was initiated by a Microsoft Teams Client

This caveat has only been applicable to SBC's deployed as Virtual Machines, or VME SBC's.

To correct this, Oracle recommends enabling Restricted Media Latching on realms configured for Microsoft Teams in the OCSBC.

The restricted media latching feature lets the Oracle® Session Border Controller latch only to media from a known source IP address, in order to learn and latch the dynamic UDP port number. The restricting IP addresses origin can be either the SDP information or the SIP message's Layer 3 (L3) IP address, depending on the configuration.

Deploying an OCSBC as a VME with Microsoft Direct routing, set this parameter to SDP.

GUI Path: media-manger/realm-config

ACLI Path: config t→media-manger→realm-config

ORACLE <sup>®</sup> Enterpr	rise Session B	order Controller				
Commands	Þ					
Media Manager	•	Modify Realm Config				
Codec Policy		Nat Trust Threshold	0	$\sim$	^	
DNS Alg Constraints		Max Endpoints Per Nat	0	$\sim$	^	
		Nat Invalid Message Threshold	0	$\sim$	^	
DNS Config		Wait Time For Invalid Register	0	$\sim$	^	
Ice Profile		Deny Period	30	~	^	
Media Manager		Session Max Life Limit	0			
Media Policy		Untrust Cac Failure Threshold	0	$\sim$	^	
Mrm Config		Subscription Id Type	END_USER_NONE		•	
waip comig		Early Media Allow				<enumeration> restricted latching mode</enumeration>
Playback Config		Enforcement Profile			•	sdp use the IP address specified in the SDP for latching
Realm Config		Additional Prefixes				Default: none
Realm Group		Restricted Latching	sdp		•	knone, sop, peer-ipx

- Click OK at the bottom
- Save and activate the configuration

## 16 Running Configuration

Below is the CLI output of show running config short. This only reflects parameters that have been modified from their default values.

11/1/2

show running-config short	
access-control	
realm-id	ATA_Realm
source-address	155.212.214.170
application-protocol	SIP
trust-level	high
access-control	
realm-id	Teams
source-address	52.112.0.0/14
destination-address	141.146.36.68
application-protocol	SIP
trust-level	nign
access-control	CIDTruck
reallin-iu	SIF ITUIK 69 69 117 67
application-protocol	SID
trust-level	high
certificate-record	ingi
name	ATACert
locality	Bedford
organization	Oracle
unit	Solutions
common-name	proxysbc.com
certificate-record	
name	BaltimoreRoot
common-name	Baltimore CyberTrust Root
certificate-record	
name	DigiCertInter
common-name	DigiCert SHA2 Secure Server CA
certificate-record	
name	DigiCertRoot
common-name	Digicent Global Root CA
name	InernalCACort
locality	Bedford
organization	Oracle
unit	Solutions
common-name	solutionslab
certificate-record	
name	TeamsEnterpriseCert
state	California
locality	Redwood City
organization	Oracle Corporation
common-name	telechat.o-test06161977.com
extended-key-usage-list	serverAuth
(	ClientAuth
codec-policy	
name	OptimizeCodecs

allow-codecs	* G722:no PCMA:no CN:no SIREN:no RED:no G729:no
add-codecs-on-egress	PCMU
codec-policy	
name	addCN
allow-codecs	*
	CN
add-codecs-on-egress	CN
atis-srtp-profile	
name	TeamsDTLS
tls-profile	TLSTeams
crypto-suite	SRTP AES128 CM HMAC SHA1 32
host-route	
dest-network	8800
notmask	255 255 0 0
netindSk	
gateway	141.140.30.03
ice-profile	
name	ice
stun-conn-timeout	0
stun-keep-alive-interval	0
local-policy	
from-address	*
to-address	*
	ATA Dealm
source-realm	ATA_Realm
	Teams
policy-attribute	
next-hop	68.68.117.67
realm	SIPTrunk
local-policy	
from-address	*
to-address	17814437247
	1781//372/18
course realm	ATA Dealm
Source-realin	
	SIPTRUIK
policy-attribute	
next-hop	SAG:TeamsGrp
realm	Teams
local-policy	
from-address	*
to-address	17814437383
	17814437384
source-realm	SIPTrunk
Source-realiti	Toome
notion officiants	
policy-attribute	
next-hop	155.212.214.170
realm	ATA_Realm
media-manager	
options	audio-allow-asymmetric-pt
	xcode-gratuitous-rtcp-report-generation
max-untrusted-signalin	α 1
min-untrusted-signaling	y . y 1
modia-profilo	
meula-prome	CN
name	
subname	wideband
payload-type	118
clock-rate	16000
media-profile	

////

21111111

name	SILK
subname	narrowband
payload-type	103
clock-rate	8000
media-profile	
name	SILK
subname	wideband
pavload-type	104
clock-rate	16000
media-sec-policy	
name	RTP
media-sec-policy	
name	sdesPolicy
inbound	
profile	SDES
mode	srtn
protocol	sdes
outbound	5005
profile	SDES
mode	orth
nrotocol	site
notwork interface	Sues
network-interface	c0p0
in address	
ip-address	141.140.30.00
netmask	200.200.200.192
gateway	141.140.30.00
dns-ip-primary	0.0.0
dns-ip-backup1	
dns-domain	
nip-ip-list	141.146.36.100
Icmp-address	141.146.36.100
network-Interface	
name	S1pU
ip-address	192.168.1.10
netmask	255.255.255.0
gateway	192.168.1.1
network-interface	
name	s1p1
ip-address	155.212.214.177
netmask	255.255.255.0
gateway	155.212.214.1
phy-interface	
name	s0p0
operation-type	Media
phy-interface	
name	s1p0
operation-type	Media
slot	1
phy-interface	
name	s1p1
operation-type	Media
port	1
slot	1
realm-config	
identifier	ATA_Realm

1/ 1

	network-interfaces		s1p1:0
	mm-in-realm	е	nabled
	media-sec-policy		sdesPolicy
	access-control-trust-level		high
	codec-policy	0	ptimizeCodecs
	realm-config		
	identifier	SIPT	runk
	network-interfaces		s1p0:0
	mm-in-realm	е	nabled
	gos-enable	en	abled
	media-sec-policy		RTP
	access-control-trust-level		high
	codec-policy	0	ptimizeCodecs
	realm-config		
	identifier	Tean	ns
	description	Re	alm Facing Teams Direct Routing
	network-interfaces		s0p0:0
	mm-in-realm	е	nabled
	gos-enable	en	abled
	media-sec-policy	•	sdesPolicy
	rtcp-mux	ena	bled
	ice-profile	ice	
	teams-fadn	te	lechat o-test16161977 com
	teams-fadn-in-uri	.0	enabled
	sdp-inactive-only		enabled
	access-control-trust-level		high
	codec-nolicy	a	1dCN
	rten-policy	rtci	Gen
	rtcp-policy		
	name	rten	Son
	rten-generate	al	
	sdos-profilo	a	realis
	sues-prome	SDE	c
			CM 100 UMAC CUA1 20
	crypto-list		0_CWI_120_NWAC_SHA1_32
	AE	.उ_∪ ว₄	VI_120_NIVIAC_SHA1_00
		SI	
	session-agent	4 5	E 040 044 470
	nostname	10	5.212.214.170
	ip-address	15	0.212.214.170
	port 5	061	
	transport-method	A <b>T</b> A	StaticiLS
	realm-id	AIA	
	ping-method	C	PTIONS
	ping-interval	30	705
	reuse-connections		ТСР
	session-agent		
	hostname	68	.68.117.67
	ip-address	68.	68.117.67
ļ	realm-id	SIP	runk
	ping-method	C	PTIONS
	ping-interval	30	
	session-agent		
	hostname	si	o.pstnhub.microsoft.com
	port 5	061	
	transport-method		StaticTLS

2/1//////

////

realm-id Teams ping-method **OPTIONS** ping-interval 30 refer-call-transfer enabled session-agent hostname sip2.pstnhub.microsoft.com port 5061 transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 30 refer-call-transfer enabled session-agent hostname sip3.pstnhub.microsoft.com 5061 port transport-method **StaticTLS** realm-id Teams ping-method **OPTIONS** ping-interval 30 refer-call-transfer enabled session-group group-name TeamsGrp sip.pstnhub.microsoft.com dest sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com sag-recursion enabled stop-sag-recurse 401,407,480 sip-config home-realm-id Teams registrar-domain registrar-host registrar-port 5060 options inmanip-before-validate max-udp-length=0 sip-message-len 0 extra-method-stats enabled sip-feature replaces name realm Teams require-mode-inbound Pass require-mode-outbound Pass sip-interface realm-id ATA\_Realm sip-port 155.212.214.177 address port 5061 transport-protocol TLS tls-profile **TLSAnalog** allow-anonymous agents-only nat-traversal rport sip-interface realm-id SIPTrunk sip-port address 192.168.1.10 allow-anonymous agents-only

secured-network	enabled
sip-interface	
realm-id	Teams
sip-port	
address	141.146.36.68
port	5061
transport-protocol	TLS
tls-profile	TLSTeams
allow-anonymous	agents-only
in-manipulationid	RespondOptions
options	100rel-interworking
sip-profile	forreplaces
sip-monitoring	
monitoring-filters	×
sip-profile	
name	torreplaces
replace-dialogs	enabled
steering-pool	
ip-address	141.146.36.68
start-port	20000
end-port	40000
realm-ld	Teams
steering-pool	
Ip-address	155.212.214.177
start-port	20000
ena-port	40000 ATA Deelm
	ATA_Realm
steering-poor	102 169 1 10
ip-address	192.100.1.10
ond-port	20000
realm-id	SIDTrunk
system-config	SIFTUIK
bostname	telechat a-test06161977 com
description	SBC for Analog and Teams
location	Burlington MA
system-log-level	NOTICE
comm-monitor	
default-gateway	10,138,194,129
source-routing	enabled
snmp-agent-mode	v1v2
tls-global	
session-caching	enabled
tls-profile	
name	TLSAnalog
end-entity-certificate	ATACert
trusted-ca-certificates	InernalCACert
cipher-list	ALL
options	ignore-root-ca=yes

///8

2111111

## tls-profile

name end-entity-certificate trusted-ca-certificates

mutual-authenticate web-server-config TLSTeams TeamsEnterpriseCert BaltimoreRoot DigiCertGlobalRootG2 enabled ///8

7/1/////

## ORACLE

CONNECT WITH US ologs.oracle.com/oracle facebook.com/Oracle/

twitter.com/Oracle

oracle.com

**Oracle Corporation, World Headquarters Worldwide Inquiries** 500 Oracle Parkway Phone: +1.650.506.7000 Redwood Shores, CA 94065, USA Fax: +1.650.506.7200

#### Integrated Cloud Applications & Platform Services

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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